RECEIVED
SEP 24 2024
Clerk, U.S. District & Bankruptcy
Courts for the District of Columbia

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Microsoft Corporation, a Washington State Corporation, NGO-ISAC, a New York State Non-Profit Organization,

Plaintiffs,

v.

John Does 1-2, Controlling A Computer Network and Thereby Injuring Plaintiff and Its Customers,

Defendants.

Case: 1:24-cv-02719 JURY DEMAND
Assigned To : Unassigned
Assign. Date : 9/24/2024
Description: TRO/PI (D-DECK)

FILED UNDER SEAL PURSUANT TO LOCAL RULE 5.1

APPLICATION OF MICROSOFT AND NGO-ISAC FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

Plaintiff Microsoft Corporation ("Microsoft") and NGO Information Sharing and Analysis Center ("NGO-ISAC") (collectively "Plaintiffs") by their attorneys, pursuant to Federal Rule of Civil Procedure 65(b) and (c), the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1116, 1125), District of Columbia common law, and the All Writs Act (28 U.S.C. § 1651) respectfully move the Court for an emergency *ex parte* temporary restraining order and order to show cause why a preliminary injunction should not issue.

As discussed in Plaintiffs' Memorandum in Support of this Application, Plaintiffs request an order transferring ownership of domains through which John Does 1-2 ("Defendants") perpetuate an unlawful spear-phishing operation, known as "Star Blizzard". The Star Blizzard Defendants are Russia-based cybercriminals, who attempt to acquire sensitive information or access computers by sending a fake email message that appears to be legitimate, with the goal of

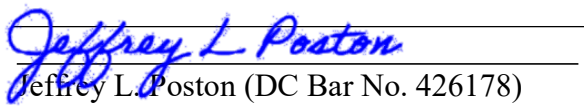
having the victim interact further with the email (referred to as the "lure"), including, for example, clicking on links in the perceived legitimate email or providing login credentials. The Star Blizzard Defendants steal confidential and personal information that they leverage to commit further cybercrimes consistent with pro-Russian interests

> The requested ex parte relief is necessary because if Star Blizzard Defendants are given advance notice, they will act to significantly impede, if not entirely preclude, Plaintiffs' ability to obtain effective relief against the Star Blizzard operation. John Does 1-2 are part of a highly technical and sophisticated cyber-criminal organization and are capable of quickly adapting the command-and-control infrastructure to avoid enforcement of the order and detection if they are given advance notice of the takedown relief sought by Plaintiffs.

Plaintiffs' Application is based on this Application, Plaintiffs' Memorandum in Support of TRO Application, the declarations of Sean Ensz (Microsoft), Ian Gottesman (NGO-ISAC), Natalia Krapiva (Access Now), Yotaro Sherman (Carnegie Corporation of New York), and Jeffrey L. Poston in support of Plaintiffs' Application and the exhibits attached thereto, the pleadings on file in this action, and on such arguments and evidence may be presented at the hearing on this Application.

Plaintiffs respectfully request oral argument on this Application be set for September 24, 2024 or as soon thereafter as the Court deems possible.

Dated: September 24, 2024



Jeffrey L. Poston (DC Bar No. 426178)
JPoston@crowell.com
Garylene Ana Joji D. Javier (*pro hac vice* pending)
GJavier@crowell.com
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington, DC 20004

Anna Z. Saber (*pro hac vice pending*)
ASaber@crowell.com
CROWELL & MORING LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111

Attorneys for Plaintiffs Microsoft Corporation and NGO-ISAC

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Microsoft Corporation, a Washington State Corporation, NGO-ISAC, a New York State Non-Profit Organization, Plaintiff, v. John Does 1-2, Controlling A Computer Network and Thereby Injuring Plaintiff and Its Customers, Defendants.	Civil Action No. **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5.1**

MEMORANDUM IN SUPPORT OF APPLICATION OF MICROSOFT AND NGO-ISAC FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

Pursuant to Rule 65 of the Federal Rules of Civil Procedure, Plaintiffs Microsoft Corporation ("Microsoft") and NGO Information Sharing and Analysis Center ("NGO-ISAC") (collectively "Plaintiffs") seek an emergency *ex parte* temporary restraining order ("TRO") and a preliminary injunction against John Does 1-2, who operate a sophisticated Russia-based, cybercriminal operation known as "Star Blizzard." The Star Blizzard Defendants have targeted and continue to target Microsoft's customers, including NGO-ISAC and its member organizations, and the general public, that work to oppose the Russian government and are adverse to Russia's interests or global and domestic policy (such as its invasion of Ukraine).

I. INTRODUCTION

Star Blizzard is a Russian-based organization that engages in spear phishing[1] through the misuse of Microsoft's trademarks and good will to access illegally the systems and data of Microsoft's customers, including NGO-ISAC. The Star Blizzard Defendants leverage this illegal access to impersonate individuals and organizations online, infiltrate email accounts, and exfiltrate-or steal- sensitive and confidential information from online accounts.

To carry out their spear phishing operation, the Star Blizzard Defendants establish and operate a network of websites, domains, and computers on the Internet, which they use to compromise the security of their victims, and steal their sensitive information. These domains comprise the Star Blizzard Defendants' "command and control infrastructure" (also referred to as a "C2 infrastructure") and are identified in **Appendix A** to Plaintiffs' concurrently filed Complaint; and also attached as **Exhibit 1** to the Declaration of Jeffrey L. Poston in Support of Plaintiffs' TRO Application ("Poston Decl.") ¶ 6.

The unlawful acts of the Star Blizzard Defendants cause great damage to Microsoft by exploiting Microsoft's famous and highly-regarded trademarks, products, and services to infiltrate email accounts. The Star Blizzard Defendants also cause immense damage to NGO-ISAC and its member organizations by impersonating the member organizations, infiltrating their email systems, and exfiltrating sensitive data related to the organizations' objectives and policy goals. These unlawful acts cause Microsoft and NGO-ISAC irreparable harm for which no monetary recourse is available or sufficient. Accordingly, Plaintiffs seek *ex parte* injunctive relief to transfer ownership of the domains that form this command and control infrastructure in order to cripple

[1] Spear phishing, as used by Plaintiffs Microsoft and NGO-ISAC in this action, is a type of personalized attack in which the threat actor or cybercriminal attempts to acquire sensitive information or access a computer by sending a fake email message that appears to be legitimate, with the goal of having the victim interact further with the email (referred to as the "lure"). *See* Declaration of Sean Ensz in Support of Plaintiffs' TRO Application ("Ensz Decl.") ¶ 5.

the Star Blizzard Defendants' ability to carry out future spear phishing attacks. Disabling these domains will cause the command and control infrastructure to be disbanded and disable the Star Blizzard Defendants' ability to carry out further attacks against Microsoft, its customers, NGO-ISAC, its member organizations, and the public.

Ex parte relief is essential. Notice to the Star Blizzard Defendants would provide them with an opportunity to destroy, move, conceal, or otherwise make inaccessible the instrumentalities they use to direct the Star Blizzard operation and the evidence of their unlawful activity. As described in Section IV.D, *infra*, Courts in numerous cases involving Microsoft have granted this form of relief to disable a cyber criminal's operation to prevent further illegal cybercrime schemes. The Court should grant the same here.

II. STATEMENT OF FACTS

A. Microsoft's Services and Reputation

Microsoft is one of the world's leading technology companies, providing complete, open, and integrated computer software programs and hardware systems. Ensz Decl. ¶ 47. Microsoft® is a provider of the Windows® operating system, and a variety of other software and services including Outlook®, OneDrive®, and Office365®. *Id.* Due to the high quality and effectiveness of Microsoft's products and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, establishing a strong brand and developing the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. *Id. Microsoft* has registered trademarks representing the quality of its products and services and its brand, including Microsoft®, Windows®, Outlook®, OneDrive®, and Office365®. Copies of the trademark registrations for these trademarks are attached as **Appendix B** to this Complaint. Microsoft's Digital Crimes Unit ("DCU") is the Microsoft division

responsible for protecting Microsoft and its customers against cybercrime threats. DCU is an international team of technical, legal and business experts that has been fighting cybercrime, protecting individuals and organizations, and safeguarding the integrity of Microsoft services since 2008.[2] One of DCU's responsibilities is to investigate cybersecurity threats and identify and attribute attacks, like it has done here with the Star Blizzard operation and Defendants. Ensz Decl. ¶¶ 2-5.

B. NGO-ISAC's Services and Reputation

NGO-ISAC is a 501(c)(3) nonprofit corporation comprised of representatives from non-governmental organizations ("NGO") that collaborate to improve the security of US-based organizations. Declaration of Ian Gottesman in Support of Plaintiffs' TRO Application ("Gottesman Decl.") ¶ 4. NGO-ISAC is focused on the cybersecurity posture of US-based nonprofits and NGOs through information sharing, training and education programs, and specialized cybersecurity consulting services, all tailored to empower and protect nonprofits. *Id.* NGO-ISAC has worked with over 200 NGOs in the United States to improve their cybersecurity. These member organizations work in important areas such as human rights, peace and disarmament, and scientific research on diseases. *Id.* ¶ 5. Each of NGO-ISAC's member organizations have cultivated reputations in their areas of practices and face cybersecurity threats such as Star Blizzard that threaten to undermine the organizations' efficacy and reputation. *Id.* ¶¶ 9, 13, 15. To serve NGO-ISAC's organizational objectives and to protect the cybersecurity of its member organizations, NGO-ISAC partner with many private sector partners, including with Microsoft. *Id.* ¶ 10.

[2] *Digital Crimes Unit: Leading the fight against Cybercime*, Microsoft, available at https://news.microsoft.com/on-the-issues/2022/05/03/how-microsofts-digital-crimes-unit-fights-cybercrime/ (May 3, 2022).

C. The John Doe Defendants Operate Star Blizzard

1. What is Star Blizzard?

The Star Blizzard Defendants are hostile, Russia-based cybercriminals that launch cyberattacks against American companies, non-profits, think tanks, information security companies, the intelligence community and individuals who are involved in foreign policy, promote anti-Russia interests, or are in positions of diplomatic significance, including former and current U.S. ambassadors and other high-ranking diplomats. Declaration of Natalia Krapiva in Support of Plaintiffs' *Ex Parte* Application for Temporary Restraining Order ("Krapiva Decl.") ¶ 14; Ensz Decl. ¶ 10. Star Blizzard's malicious and criminal activities are carried out by John Does 1-2. Ensz Decl. ¶ 10.

The Star Blizzard Defendants' campaigns in recent years have targeted over 30 organizations, in addition to personal accounts of individuals. The Star Blizzard Defendants primarily targets organizations and individuals in NATO countries, particularly the US and the UK, with occasional targeting of entities in other countries in the Baltics, the Nordics, and Eastern Europe. *Id.* For instances, the Star Blizzard Defendants targeted the government sector of Ukraine in the months leading up to the invasion by Russia, and Western governments and NGOs opposed to Russia's invasion. *Id.*

2. The Star Blizzard Defendants' *Modus Operandi*

Star Blizzard employs spear phishing to perpetrate their attacks. Ensz Decl. ¶ 5. Spear phishing is a type of personalized attack in which the cybercriminal attempts to acquire sensitive information or access a computer by sending a fake email message that appears to be legitimate, with the goal of having the victim interact further with the email (referred to as the "lure"). *Id.* ¶¶ 5-6. The Star Blizzard Defendants engineer these emails to deceive their victims into thinking that they are responding to a legitimate email and to trick them into opening a malicious link or

attachment or providing sensitive information, including credentials or confidential information. *Id.* ¶ 15. In doing so, the Star Blizzard Defendants aim to gain unfettered access and control of the victim's inbox, so that it can commit further cybercrimes largely against organizations that work to oppose the Russian government and are adverse to Russia's interests or global and domestic policy (such as its invasion of Ukraine). *Id.* This includes the Star Blizzard Defendants targeting former U.S. Ambassador to Ukraine, Steven Pifer. Krapiva Decl. ¶ 14.

The Star Blizzard Defendants have built a command and control infrastructure involving a network of website domains. Ensz Decl. ¶ 54. A website domain is also known as a web address and is used to identify a website and allow users on the internet to access the website. These website domains are identified in **Appendix A** to the Complaint. *Id.*; Poston Decl. ¶ 6, Ex. 1.

The Star Blizzard Defendants use these domains to carry out these attacks by (1) impersonating known contacts' email accounts, (2) creating fake social media profiles, (3) using email address from providers such as Outlook (to increase the appearance of "legitimacy" and to purposefully mislead the victim into thinking that an email from Microsoft account is benign and legitimate), and (4) creating malicious domains that resemble legitimate organizations (such as Microsoft, NGO-ISAC, or the NGO-ISAC member organizations). Ensz Decl. ¶¶ 15-20; Gottesman Decl. ¶¶ 14-17. Plaintiffs bring this action to take down this technical infrastructure and render the Star Blizzard Defendants incapable of continuing their attacks. Ensz Decl. ¶¶ 54-62; Gottesman Decl.¶¶ 18-19.

The Star Blizzard Defendants leverage Microsoft systems and programs, such as Outlook, Office365, or OneDrive to further increase the perceived legitimacy of the attack. In doing so, the Star Blizzard Defendants capitalize and misuse the brand recognition that Microsoft has cultivated and the trust Microsoft has built with its customers. Ensz Decl. ¶ 47.

3. The Star Blizzard Defendants' Attack Chain

A Star Blizzard attack begins with online reconnaissance efforts of publicly available information to identify targets, which includes scouring social medial platforms, networking platforms, organization contact lists, and other public facing sources of intelligence. Ensz Decl. ¶¶ 15-18. The purpose of these reconnaissance efforts is to capture information that the Star Blizzard Defendants can use to craft a personalized spear phishing email. *Id. The* social engineering involved exploits the target's human psychology, rather than technological vulnerabilities. Gottesman Decl. ¶ 14. By way of explanation, if the Star Blizzard Defendants are trying to attack an NGO-ISAC member organization, they will have more success if the target believes they are emailing with an industry colleague. *Id.* So, reconnaissance in this circumstance would identify industry events and then send an email to the target pretending to have attended that industry event—(*i.e.*, an outreach email based on reconnaissance efforts that demonstrate that the target spoke at a panel: "Thank you for speaking at the panel, I would like to talk more about your presentation") are more likely to engender a response compared to a generic phishing email that is not personalized. *Id*.

Another example of a reconnaissance effort is identifying individuals in a target's network. This would allow the Star Blizzard Defendants to send an introduction email such as "I received your name from [contact in target's network], and they recommended I reach out because you are the subject matter expert in a field I am also interested in." Ensz Decl. ¶¶ 15, 21. Because this reconnaissance is the prerequisite for sending a targeting and personalized spear phishing email—rather than some generic attempt—these efforts are necessary to effectively carry out a successful spear phish, otherwise the spear phishing email may go ignored. Gottesman Decl. ¶ 14.

Once the operation identifies a target, the Star Blizzard Defendants then begin the next

phase of their attack: using various consumer email provider (such as Microsoft-owned Outlook) to sign up or open a new email account to act as the sender of the spear phishing email to the target. Ensz Decl. ¶¶ 19-21. To do this, the Star Blizzard Defendants will register new email accounts at various consumer email providers, such as Microsoft-owned Outlook. *Id.* ¶ 19. Star Blizzard intentionally designs these registered email addresses to match or look similar to legitimate email addresses and account names. *Id.* An example of this would be misspelling a name by one letter so that the target does not catch the difference: using "5" instead of "s" or "nn" instead of "m." Because the fake email addresses often go undetected, the Star Blizzard Defendants are able to reuse these accounts. *Id.* ¶ 20. If detected, the Star Blizzard Defendants simply create new email accounts that appear to look legitimate. *Id.*

The next step is the actual delivery of the spear phishing email. Ensz Decl. ¶¶ 19-28. The Star Blizzard Defendants use these impersonated accounts to establish contact with the target. *Id.* ¶ 21. The communication appears legitimate, and the Star Blizzard Defendants develop rapport with the victim, who is then more likely to further the interaction. *Id.* If the target responds, the rapport building then escalates to the sending of a fictitious attachment. *Id.* **FIGURE 1**, below, depicts an actual example of a Star Blizzard-initiated spear phishing email. Ensz Decl. ¶ 21.

I shared the paper. Did you get it?

Cheers,

[redacted]

From: [redacted]
Sent: [redacted]
To: [redacted]@outlook.com>
Subject: Re: Wondering what you guys think

Please send the attachment

Get Outlook for iOS

From: [redacted]@outlook.com>
Sent: Tuesday, June 8, 2021 8:53:41 AM
To: [redacted]
Subject: Re: Wondering what you guys think

[redacted]

I know you have your hands full at the moment, but nevertheless thought this would interest you (attached).

FIGURE 1

In this example, the correspondence begins with the sender sharing an article of interest and acknowledging that the recipient is busy. Because the victim does not suspect that this email is a lure, they respond and further engage in the conversation, asking the sender to share the attachment. The Star Blizzard Defendants (the purported sender) then send a follow up confirming that they shared the requested paper. It is at this point that Defendants attach a file or includes a link to a file share platform like OneDrive. Ensz Decl. ¶¶ 24-28. The secondary email (containing the file or the link) is the weaponized email, which is the email that is integral to the spear phishing effort. *Id.* The goal of the Star Blizzard Defendants are for the target to open the document or click on the link. *Id.*

Sometimes, as in the example above, the sender will be someone external to the target's organization; in other instances, the Star Blizzard Defendants will impersonate a manager of a particular organization and will use the "sender's" authority to lure the recipient into opening a link. Ensz Decl. ¶¶ 12-22. These spear phishing emails would be addressed to the sender's "colleagues," would reference internal practices, that leads the recipient to believe that the lure is a legitimate email coming from a manager. *Id.*

The Star Blizzard Defendants use different methods to deliver a document that encourages the recipient to interact with the document and/or the link contained within: (1) including a link to the document in the body of an email, (2) attaching a PDF file that contains a link, or (3) sending OneDrive link to a PDF file. Ensz Decl. ¶¶ 24-28. Each of these methods encourage the same end result: the victim clicks on the link, which redirects them to a domain controlled by the Star Blizzard Defendants, and then unsuspectingly enters login credentials to its Microsoft account. *Id.* In each instance the Star Blizzard Defendants use tactics such as impersonating and imitating a OneDrive file or other file sharing platform, request the victim to open the document by click

multiple buttons (each of which can redirect the victim to a Star Blizzard-controlled domain), or claiming that there is an "error" with preview so that the victim must actually open the document to see the attachment. *Id.* If the recipient is expecting an email with an attachment (this is why the "benign" rapport building at the outset regarding shared interests is critical), they will not be suspicious of a link or an attachment (the way a recipient may be suspicious if they receive the attachment out of the blue). *Id.* Regardless of the method of delivery of the file, when the target clicks the link, the link redirects them to a Star Blizzard-controlled domain, which means that the Star Blizzard Defendants have access to whatever information a victim enters onto that website. Ensz Decl. ¶ 28.

After clicking on the redirect link, the Star Blizzard Defendants present the victim with a webpage that *appears* to be a Microsoft login page (for example, an Outlook or Office365 login page), but in reality, it is a spoofed page that the Star Blizzard Defendants control. *Id.* ¶¶ 29-33, 40. The recipient of the spear phishing email, thinking that the login page is a legitimate Microsoft login page to access their account, will enter their login credentials. *Id.* Once redirected to the login page, the framework prompts the target for authentication, mirroring the sign-in page for a legitimate provider, allowing the Star Blizzard Defendants to intercept any credentials. *Id.* Once a victim inputs their login credentials, the Star Blizzard Defendants are able to capture the credential (as well as any two-factor authentication that the account may have implemented, *e.g.*, login credentials as well as a one-time code sent to an email address connected with that username and password). Ensz Decl. ¶¶ 31-33. To avoid detection, the Star Blizzard Defendants further redirect the victim to a website or document (*e.g.*, the "document" that was the lure for the attack) so that the target remains unaware that they have been compromised. *Id.* ¶ 33.

Once the victim enters the credentials, the next step is data exfiltration. *Id.* ¶¶ 34-35. In

some cases, the Start Blizzard Defendants can take advantage rules (such as a forwarding rule) that would automatically forward an email received by the victim to another email address (in this case, a Star Blizzard-owned email address). *Id.* ¶ 34. By setting up automatic forwarding rules, the Star Blizzard Defendants ensure that they have long-term access to the exfiltrated data. *Id.* In other cases, the Star Blizzard Defendants have been able to use its persistent access to the inbox, to exfiltrate mailing lists and other contact information to continue the scheme. *Id.* The Star Blizzard Defendants are able to later use the credentials to access the victims' email account, and leverage that access and the data stolen from those accounts to launch additional cybercrimes. Ensz Decl. ¶¶ 34-35; Gottesman Decl. ¶¶ 12-13, 15-17.

D. Harm to Microsoft and NGO-ISAC

The Star Blizzard Defendants have affirmatively targeted Microsoft customers in the United States, specifically the Washington, D.C. area. Ensz Decl. ¶¶ 44-45. To carry out their criminal operation, the Star Blizzard Defendants use Microsoft based software and services. *Id.* ¶ 29 (Star Blizzard spear phishing email may include a link to a OneDrive file, which is fabricated to appear legitimate, enticing the target to click on the link, which appears as a Microsoft login page). If the victim uses OneDrive regularly, they will be unsuspecting that a link to a purported OneDrive document is malicious or compromised; indeed, the victim may believe that the link has been "vetted" by Microsoft's cybersecurity software. *Id.*. The Star Blizzard Defendants' use of Microsoft brands and trademarks is meant to confuse Microsoft's customers into clicking on malicious links that they believe are associated with and owned by Microsoft. Ensz Decl. ¶ 47. When the victim realizes that they have been attacked, they hold Microsoft responsible for or complicit in the attack and customers may incorrectly attribute these problems to Microsoft's products and services, thereby diluting and tarnishing the value of these trademarks and brands.

Id. ¶¶ 49, 51.

Likewise, the Star Blizzard Defendants damage NGO-ISAC and its member organizations through impersonation campaigns. Ensz Decl. ¶ 52; Gottesman Decl. ¶¶ 15-17. The Star Blizzard Defendants' impersonation, credential theft, and exfiltration of sensitive data are particularly damaging, as it can impact the targeted victim's career and reputation, as well as the reputation of the NGO the victim is associated with and the overall efficacy of the NGO's policy work objective. Ensz Decl. ¶¶ 52-53. For example, Carnegie Corporation of New York is an NGO-ISAC member organization[3], that has been targeted by the Star Blizzard Defendants. Gottesman Decl. ¶ 15; Declaration of Yotaro Sherman in Support of Plaintiffs' TRO Application ("Sherman Decl.") ¶¶ 7-14. The Star Blizzard Defendants impersonated Carnegie Corporation of New York's grant program and through the impersonation efforts sent additional spear phishing emails to grantees. Gottesman Decl. ¶ 15; Sherman Decl. ¶¶ 9-11. In these emails, "Carnegie Corporation of New York" informed the target that reporting related to their grant was overdue[4] and they would need to login in to complete the reporting. Sherman Decl. ¶ 10. The email also included a link to the "login" page that masked itself as a legitimate login page for Carnegie Corporation's grant portal, and referenced "Carnegie Fluxx," which is the name of the portal used by Carnegie Corporation. *Id.* ¶ 9. In addition to causing confusion amongst the spear phishing targets, as many believed the impersonation emails to be legitimate, the Star Blizzard Defendants were able to capture login

[3] Carnegie Corporation issues grants as part of its program on International Peace and Security, including for research and analysis of Russia foreign and domestic policy. As part of Carnegie Corporations's focus on Russia-related issues, Carnegie Corporation has authored a report analyzing how Russia's invasion of Ukraine has adversely affected US-based Russian Studies efforts. Sherman Decl. ¶ 1, n. 1; Wilfred Chan, *How Russian Studies Is Grappling with the War in Ukraine*, Carnegie Corporation of New York, available at https://www.carnegie.org/our-work/article/how-russian-studies-is-grappling-with-the-war-in-ukraine/ (May 3, 2024).

[4] If a grantee has an overdue report related to one grant, they will not be able to obtain grant money funds related to a different.

credential that would give Defendants access to sensitive information concerning project-specific grants. *Id.* ¶¶ 10, 13-14. The Star Blizzard Defendants attacks have required NGO-ISAC's member organizations to commit resources to their data and network security. Gottesman Decl. ¶ 16. NGO-ISAC has also focused resources on victims of Star Blizzard attacks who are both impersonated as part of these campaigns and targeted by these impersonations as part of spear phishing campaigns. *Id.* ¶ 17. Many of these victims are former US Government officials who now work at NGOs on issues that are adverse to Russia's global and domestic policy objectives. *Id.* When successful, these spear phishing threats can lead to time consuming and costly remediation efforts. For example, victims are forced to change bank accounts that were tied to compromised emails, struggle to get personal information removed from the internet, must work with their network of peers to alert others to the issue, and create new email accounts. *Id.* As a result of the spear phishing and impersonation campaign of the Carnegie Fluxx grant portal by the Star Blizzard Defendants, Carnegie Corporation had to expend resources to notify 2,600 grantee contacts of the attack and warn them that the emails they received were not legitimate. Sherman Decl. ¶ 15. Even when these campaigns do not successfully breach accounts, they slow down victims' ability to work, eroding trust within the attacked communities, making their work harder and less effective. Gottesman Decl. ¶ 17.

III. LEGAL STANDARD

Federal Rule of Civil Procedure 65 authorizes the court to grant a temporary restraining order and preliminary injunction when the moving party demonstrates that absent such relief it will endure immediate and irreparable injury. Fed. R. Civ. P. 65(b). The purpose of a preliminary injunction is to protect the status quo and to prevent irreparable harm during the pendency of a lawsuit and to preserve the court's ability to render a meaningful judgment on the merits. *Gold v.*

State Plaza, Inc., 435 F. Supp. 2d 110, 119 (D.D.C. 2006) (finding an order maintaining the status quo "is appropriate when a serious legal question is presented, the public interest is served, denial of the requested relief would inflict irreparable injury on the movant and when little if any injury would befall the respondent"). A plaintiff must show: (1) that it "is likely to succeed on the merits;" (2) that it "is likely to suffer irreparable harm in the absence of preliminary relief;" (3) "that the balance of equities tips in [its] favor;" and (4) "that an injunction is in the public interest." *Robert Half Int'l Inc. v Billingham*, 315 F. Supp. 3d 419, 426 (D.D.C. 2018) (quoting *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7 (2008)). "[I]t is generally recognized that 'trademark infringement by its very nature causes irreparable injury." *Breaking the Chain Found., Inc. v. Capitol Educ. Support, Inc.*, 589 F. Supp. 2d 25, 30 (D.D.C. 2008) (granting permanent injunction and noting "Defendant's continuing disregard for Plaintiffs rights" and "public interest favors protecting against further violation of federal trademark laws").

IV. PLAINTIFFS' REQUESTED RELIEF IS WARRANTED.

As described herein, there is a very high likelihood that Plaintiffs will succeed on the merits. Plaintiffs, their customers, member organizations, and the public will continue to be irreparably harmed if the Star Blizzard Defendants are able to continue their cybercriminal operation. Every day that passes gives the Star Blizzard operation further opportunity to carry out additional spear phishing attacks, steal email credentials, and invade the privacy of the victims' email inboxes. Unless enjoined, the Star Blizzard Defendants will continue to irreparably harm Plaintiffs. Plaintiffs' requested relief is warranted because the effect on third parties (such as domain registries) will be negligible and temporary. Comparatively, if a TRO and preliminary injunction are issued, no legitimate interest of Star Blizzard Defendants will be harmed—indeed, they do not have *any* legitimate interest that would allow them to continue committing cybercrime.

Finally, the public interest also weighs heavily in favor of relief because the same injury inflicted on Plaintiffs and their customers by the Star Blizzard Defendants affect the public, because they too are victims of the Star Blizzard Defendants' criminal activity. Accordingly, this matter presents a quintessential case for injunctive relief.

A. Plaintiffs Are Likely to Succeed on the Merits.

Plaintiffs are likely to succeed on the merits of their claims and as such, their request for a TRO and a preliminary injunction should be granted. Plaintiffs' Complaint sets forth the following statutory and common law claims: violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030); violations of the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 et seq.); and the common law claims of trespass, conversion, and unjust enrichment. Even at this early stage in the proceedings, the record demonstrates that Plaintiffs will be able to establish the elements of each of their claims. The evidence in support of Plaintiffs' TRO application is based on the diligent work of experienced investigators and is supported by substantial empirical evidence and forensic documentation. In short, there is no legitimate dispute about what the Star Blizzard Defendants do and the damage they cause. Given the strength of Plaintiffs' evidence, the likelihood of success on the merits weighs heavily in favor of granting injunctive relief.

1. The Star Blizzard Defendants Violate the Computer Fraud and Abuse Act

Congress enacted the Computer Fraud and Abuse Act (the "CFAA") specifically to deter hacking and to address computer crime. *See, e.g.*, *Lewis-Burke Assocs., LLC v. Widder*, 725 F. Supp. 2d 187, 194 (D.D.C. 2010); *Hedgeye RiskMgmt., LLC v. Heldman*, 271 F. Supp. 3d 181, 195 (D.D.C. 2017) (discussing criminal aspects of CFAA which is designed to target "hackers").

Inter alia, the CFAA penalizes a party that intentionally accesses a protected computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer. 18 U.S.C. § 1030(a)(2)(C).

A "protected computer" is a computer "used in interstate or foreign commerce or communication. *Human Touch DC, Inc. v. Merriweather*, 2015 WL 12564166, at *4 (D.D.C. May 26, 2015) (finding "computers connected to the internet are part 'of a system that is inexorably intertwined with interstate commerce'").

The phrase "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled to obtain or alter." 18 U.S.C. § 1030(e)(6). This includes password or credential theft in order to access an account that the defendants would otherwise not have authorization to access. *Psychas v. Dist. Dep't of Transportation*, 2019 WL 4644503, at *5 (D.D.C. Sept. 24, 2019).

Although a criminal statute, the CFAA also provides a private cause of action for any person "suffer[ing] damage or loss" from a violation of the act, if the plaintiff demonstrates loss or damage in excess of $5,000. 18 U.S.C. § 1030(g). The CFAA defines loss as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program. system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11); *Human Touch*, 2015 WL 12564166, at *4 (plaintiff met $5,000 requirement where plaintiff spent "more than $5,000 in resources and personnel hours, including hiring legal counsel, to remedy Defendant's unauthorized access and taking."). "The CFAA . . .permit[s] plaintiffs to aggregate multiple intrusions or violations for the purposes of meeting the $5,000 statutory threshold." *See Sprint Nextel Corp. v. Simple Cell, Inc.*, 2013 WL

3776933, at *7 (D. Md. July 17, 2013) (citations omitted).

In sum, to prevail on their CFAA claim, Plaintiffs must establish that the Star Blizzard Defendants accessed a protected computer, without authorization, for the purpose of obtaining information or defrauding others, which resulted in loss or damage in excess of $5,000. The Star Blizzard Defendants use spear phishing and credential theft to gain access to the victims' computers and networks without permission—indeed, the Star Blizzard Defendants spear phishing attacks *trick* victims into sharing login credentials. *See* Ensz Decl. ¶¶ 15-33. Once the Star Blizzard Defendants have obtained credentials through ill-gotten means, they exfiltrate sensitive data from victims. *Id.* ¶ 34. In other instances, the Star Blizzard Defendants *impersonates* a trusted NGO-ISAC member organization in order access the victims' computers without authorization. Gottesman Decl. ¶¶ 15-16; *see also* Krapiva Decl. ¶¶ 10, 18, 20, 30. The Star Blizzard Defendants' conduct is precisely the type of activity that the CFAA is designed to prevent. *Human Touch*, 2015 WL 12564166, at *4, *6 (granting preliminary injunction under CFAA based on allegations of defendant's "unauthorized removal of [plaintiffs] patients' confidential health information"). As a result of the Star Blizzard Defendants' unlawful actions, Plaintiffs have incurred more than $5,000 in damages. Ensz Decl. ¶ 47; Gottesman Decl. ¶ 16. To date, Microsoft has incurred approximately $1,000,000, which represents personnel costs involved in investigative and remediation efforts. Ensz Decl. ¶ 47. Since 2023, Carnegie Corporation as just one NGO-ISAC member organization, had to expend approximately $200,000 to investigate and remediate harm caused by the Star Blizzard Defendants. Yotaro Decl. ¶ XX. Other NGO-ISAC member organizations have also incurred similar damage. Gottesman Decl. ¶ 16.

2. The Star Blizzard Defendants Violate the Electronic Communication Privacy Act

The Electronic Communications Privacy Act ("ECPA") prohibits "intentionally

access[ing] without authorization a facility through which electronic communications are provided" or doing so in excess of authorization, and, in so doing, obtaining, altering, or preventing authorized access to an electronic communication while it is in electronic storage. 18 U.S.C. § 2701(a). ECPA is violated when defendant logs into plaintiff's account without permission (including with stolen credentials) and intentionally accesses the contents of an inbox. *McPherson v. Harker*, 2021 WL 1820290, at *11 (D.D.C. May 6, 2021) (husband violated ECPA "when he 'intentionally access[ed]' Facebook's servers, by logging into his wife's account without her permission, in order to 'obtain[ ] ... a[n] electronic communication,' namely the Facebook messages between Mrs. Thomas and plaintiff, in 'electronic storage' on those servers) (alteration in original).

The Star Blizzard Defendants' conduct in carrying out their criminal objectives violates the ECPA because they break into computer networks through the use of ill-obtained passwords with the direct intention of acquiring the contents of the victims' email inbox and exfiltrating sensitive business or personal information. *See* Ensz Decl. ¶¶ 34-35 (the Star Blizzard Defendants routinely use stolen credential to sign into victim accounts to engage in data exfiltration—including, both the access and viewing of emails, attachments to those emails, and contact lists—which is a key objective of the Star Blizzard operation). *Id*.; Gottesman Decl. ¶¶ 6, 11. Through this unauthorized access, the Star Blizzard Defendants intercepted, had access to, obtained and altered, and/or prevented legitimate, authorized access to, wire and electronic communications transmitted through the computers and infrastructure of NGO-ISAC member organizations and its users. Gottesman Decl. ¶ 15. For example, upon a successful spear phish, the Star Blizzard Defendants were able to obtain unique grant numbers associated with a member organization's grant issuing process to appear as though Defendants' subsequent spear phishing emails were

authentic and sent by Carnegie Corporation of New York, an NGO-ISAC member organization. *Id.*; Sherman Decl. ¶ 17.

Obtaining stored electronic information in this way, without authorization, is a per se violation of ECPA. *See Council on Am.-Islamic Relations v. Gaubatz*, 667 F. Supp. 2d 67, 71-73 (D.D.C. 2009) (granting preliminary injunction in case where plaintiff brought ECPA claims after defendant removed 12,000 internal, sensitive documents including emails and other documents and made video and audio recordings of private meetings and published this information); *Human Touch*, 2015 WL 12564162, at *2 (plaintiff likely to succeed on merits for purpose of TRO where defendant accessed Capitol View's email system without authorization for purpose of accessing sensitive communications and patient information). Thus, Plaintiffs are likely to succeed on the merits of their ECPA claims.

3. The Star Blizzard Defendants Violate the Lanham Act

Section 1114 of the Lanham Act prohibits use of a reproduction, counterfeit, copy or "colorable imitation" of a registered mark in connection with the distribution of goods and services where such use is likely to cause confusion or mistake or to deceive. *Am. Ass'n for Advancement of Sci. v. Hearst Corp.*, 498 F. Supp. 244, 259-61 (D.D.C. 1980).

The Star Blizzard Defendants misuse Plaintiffs' registered, famous. and distinctive trademarks in a number of fraudulent ways. They reproduce Microsoft trademarks such as "Microsoft," "Windows," Outlook," and "OneDrive" and reproduce trademarks of NGO-ISAC member organizations, such as "Carnegie Corporation of New York[5]" in phishing e-mails in a

[5] NGO-ISAC has associational standing as representative of its members because (1) multiple NGO-ISAC members would otherwise have standing to sue in their own right, (2) the interests of NGO-ISAC as an association seeks to protect in this action are germane to the organization's purpose and (3) as NGO-ISAC seeks only equitable relief, neither the claim asserted nor the

manner that is intended to induce the recipient of the phishing e-mail into trusting the legitimacy of the email. Ensz Decl. ¶¶ 29, 47; Gottesman Decl. ¶¶ 15; Sherman Decl. ¶¶ 12, 16. For example, **FIGURE 2** is a screenshot from a Star Blizzard spear phishing email where Defendants use the "OneDrive" and "Microsoft" logos to manufacture legitimacy.

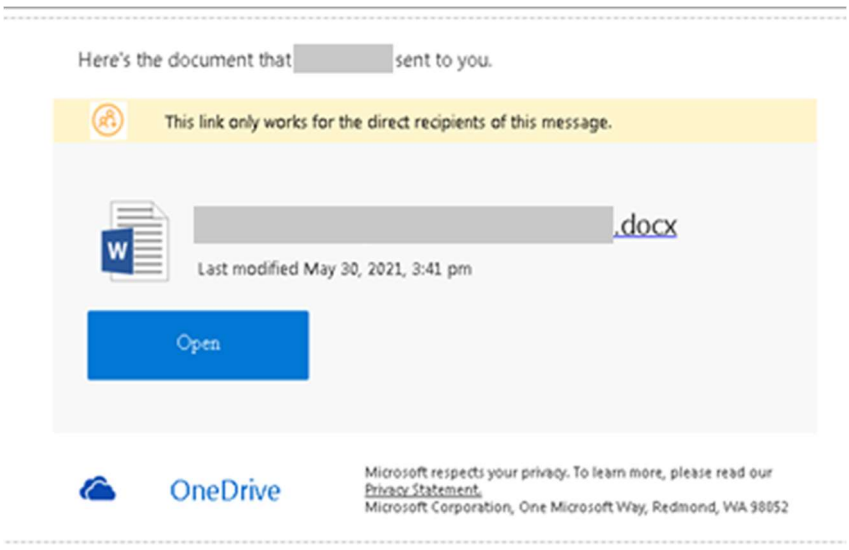


FIGURE 2

Similarly, **FIGURE 3** is a screenshot of a Star Blizzard spear phishing email where the Star Blizzard Defendants were impersonating Carnegie Corporation of New York, an NGO-ISAC member organization. Sherman Decl. ¶ 12, Exhibit 2. The name "Carnegie Corporation of New York" has been trademarked (*see* Complaint, Appendix C), and an email impersonating Carnegie Corporation caused confusion, as recipients believed the email to actually be from Carnegie Corporation and related to "Carnegie Fluxx," which is Carnegie Corporation's grant management system. *Id.*

---

relief requested requires participation of individual members in this action. *Hunt v. Washington State Apple Advert. Comm'n*, 432 U.S. 333, 343 (1977). Accordingly, NGO-ISAC has standing to assert claims for violation of the Lanham Act on behalf of Carnegie Corporation of New York, one if its member organization.

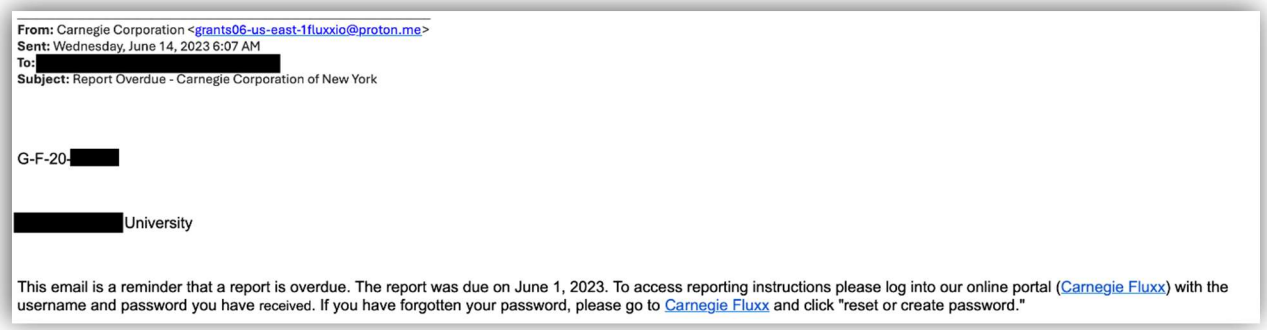


FIGURE 3

Likewise, when a victim redirected to the final page, the target is prompted to enter their credentials, by proxying the connect to the sign-in page for a legitimate provider and intercepting any credentials and authentication tokens. **FIGURE 4** depicts an example of a cloned phishing portal used by the Star Blizzard Defendants to directly impersonate a victim organization. Ensz Decl. ¶¶ 32-33.

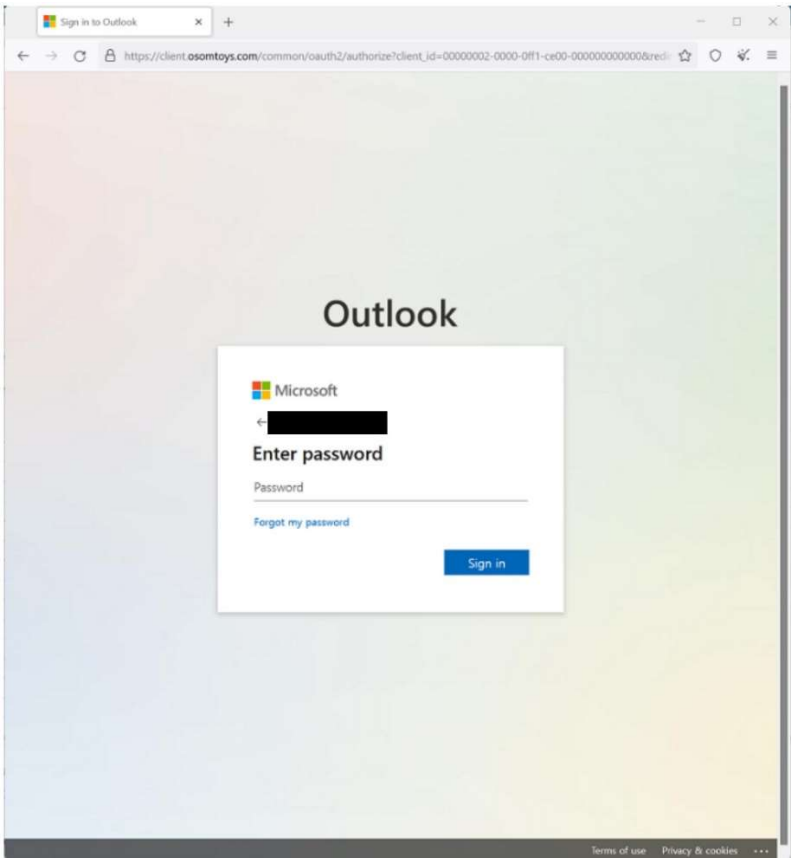


FIGURE 4

The Star Blizzard Defendants' creation and use of counterfeit trademarks in connection with such fraud is likely to cause confusion and mistake, and likely deceive consumers.

This is a clear violation of the Lanham Act. Indeed, "[a]n alternative, although unnecessary, means of showing likelihood of confusion is by the presumption that proof of wrongful intent on the part of the defendant raises." *Hearst Corp.*, 498 F. Supp. at 260; *Marquis Who's Who, Inc. v. N. Am. Advert. Assocs., Inc.*, 426 F. Supp. 139, 142 (D.D.C. 1976) (focusing on intent and noting "[d]efendants were aware of Plaintiff's mark when their title was chosen and their intent in choosing that title appears to have been to trade upon Plaintiffs established reputation and goodwill").

The Star Blizzard Defendants' conduct also constitutes false designation of origin under section 1125(a), which prohibits use of a registered mark that "is likely to . . . deceive as to the affiliation, connection, or association of such person . . . or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities." 15 U.S.C. § 1125(a)(1)(A). The Star Blizzard Defendants' misleading use of Plaintiffs' marks causes confusion and mistake as to Plaintiffs' affiliation with the Star Blizzard Defendants' malicious conduct. For example, when a target is directed to a "Microsoft login screen," the target believes it is actually entering its Microsoft credentials. Ensz Decl. ¶¶ 32-33. Similarly, when a target receives a spear phishing email from an email address impersonating an NGO-ISAC member organization email address, the target believes it is actually receiving an email from the member organization, and not a cybercriminal. When the Star Blizzard Defendants impersonated Carnegie Corporation's grant system, recipients of the email were led to believe this was legitimate communication regarding a grant they had applied for and were unsuspecting that the Star Blizzard Defendants were actually unlawfully leveraging the trademarks and branding of NGO-ISAC member organizations.

Gottesman Decl. ¶ 15; Sherman Decl. ¶ 13. This activity is a clear violation of Lanham Act under § 1125(a), and Plaintiffs are likely to succeed on the merits. *See Hearst Corp.*, 498 F. Supp. at 261 (granting injunctive relief after finding [w]ithout doubt [defendant's] new version of Science Digest is likely to be confused with, and therefore infringes, AAAS's valid trademark "Science" and noting "[i]t is 'stretching credulity beyond its breaking point' to suppose that a defendant would not have familiarized himself with the brands and names under which his competitor does business"). Indeed, the Star Blizzard Defendants have every motivation to copy Plaintiffs' marks as much as possible in order to carry out a more effective spear phish. *Sears, Roebuck & Co. v. Sears Fin. Network*, 576 F. Supp. 857, 864 (D.D.C. 1983) (granting preliminary injunction on trademark infringement claims involving 'SEARS" name and inferring intent to trade off the well-known "SEARS" name); *N. Am. Advert. Assocs., Inc.*, 426 F. Supp. at 142-43 (granting permanent injunction after finding for plaintiff on trademark infringement claim).

These are clear violations of the Lanham Act, and Plaintiffs are likely to succeed on the merits.

4. The Star Blizzard Defendants' Conduct is Tortious

The Star Blizzard Defendants' conduct is tortious under the common law doctrines of conversion, trespass to chattels, and unjust enrichment.

Conversion

Conversion, under District of Columbia law, is "any unlawful exercise of ownership. dominion or control over the personal property of another in denial or repudiation of his rights thereto." *Yung v. Institutional Trading Co.*, 693 F. Supp. 2d 70, 80 (D.D.C. 2010); *Yah Kai World Wide Enters., Inc. v. Mapper*, 195 F. Supp. 3d 287, 325 (D.D.C. 2016) (defendants liable for converting intangible property rights of plaintiff in the form of computer records). Here, the Star

Blizzard Defendants stole email account credentials and then used the credentials to access email accounts and steal sensitive data contained within the victims' inboxes. Additionally, the Star Blizzard Defendants exercised dominion and authority over the infiltrated inboxes, including impersonating the victims to spear phish the victims' contacts and having the ability to set up email inbox rules (for example, setting up a forwarding rule such that any time the victim receives an email it is automatically forwarded to a Star Blizzard-controlled email address to maintain long-lasting access). Ensz Decl. ¶ 34. This is quintessential conversion. *Ground Zero Museum Workshop v. Wilson*, 813 F. Supp. 2d 678, 697 (D. Md. 2011); *Kremen v. Cohen*, 337 F.3d 1024, I 034 (9th Cir. 2003) (hacking into computer system and injuring data supports a conversion claim).

Trespass to Chattels

Courts have found trespass to chattels where a party intentionally uses or interferes with personal property in rightful possession of another without authorization. *Physicians Interactive v. Lathian Sys., Inc.*, 2003 WL 23018270, at *9 (E.D. Va. Dec. 5, 2003) (E.D. Va. 2003) (TRO and preliminary injunction where defendant hacked computers and obtained proprietary information). The Star Blizzard Defendants' actions in operating the command and control infrastructure constitute trespass to chattels by using Microsoft services to carry out their illegal spear phishing. Additionally, their conduct results in the unauthorized access to the network infrastructure of NGO-ISAC's member institutions, and result in unauthorized intrusion into those computers and theft of information and account credentials. For example, the Star Blizzard Defendants' tortious misuse proprietary Microsoft services and software to carry out the attacks constitutes trespass to chattel because Microsoft is deprived of the ability to control how its software and services are used. Ensz Decl. ¶ 44. Likewise, the Star Blizzard Defendants are liable

for the tort of trespass to chattels when they hack and exfiltrate data related to grant numbers from Carnegie Corporation to further carry out attacks. Courts in this circuit have expressly found that computer hacking constitutes trespass to chattel. *Jones v. United States*, 168 A.3d 703, 717 (D.C. 2017); *Matter of Search of Info. Associated with [Redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.*, 13 F. Supp. 3d 145, 151 (D.D.C.), *vacated on other grounds by Matter of Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.*, 13 F. Supp. 3d 157 (D.D.C. 2014) (trespass to chattels when data is copied without authorization). Additionally, this conduct has been found to be a trespass to chattels in other cases involving similar cyberattacks against Microsoft and its customers. *E.g.*, *Microsoft Corp. v. Does 1-18*, 2014 WL 1338677, at *9-10 (E.D. Va. Apr. 2, 2014) (finding plaintiff alleged sufficient facts on conversion and trespass to chattel claims to where defendant accessed computers and servers associated with Microsoft's Internet Explorer, Bing, and Bing Ads without authorization and engaged in click-fraud by directing web browser sessions and search engine results to websites of defendant's choice).

The elements of an unjust enrichment claim are "(1) the plaintiff conferred a benefit on the defendant; (2) the defendant retains the benefit; and (3) under the circumstances, the defendant's retention of the benefit is unjust." *Falconi-Sachs v. LPF Senate Square, LLC*, 142 A.3d 550, 556 (D.C. 2016). The Star Blizzard Defendants, who are cybercriminals, have been unjustly enriched through their unlawful use of Plaintiffs' trademarks, brand names, goodwill, goods, and services to carry out spear phishing cyber-attacks. Plaintiffs' have spent considerable resources to develop their brands, such that their customers and the public trust their branding and reputation. Ensz Decl. ¶¶ 47-49. In order to ensure greater efficacy of the Star Blizzard Defendants' spear phishing activities, the Star Blizzard Defendants usurp this good will and reputation so that the spear phish

victim is more likely to interact with the lure. *Id.* ¶¶ 21-22. Moreover, once the Star Blizzard Defendants infiltrate the victims' inbox, the theft of sensitive information further unjustly enriches the Star Blizzard Defendants and it is inequitable for Defendants to retain these benefits.

Accordingly, Plaintiffs will succeed on each of their tort claims.

B. The Star Blizzard Defendants Cause Irreparable Harm.

The Star Blizzard criminal operation causes harm that is unlikely to ever be compensated—even after final judgment—because the Star Blizzard Defendants are elusive cybercriminals whom Plaintiffs are unlikely to be able to enforce judgments against. This District recognizes "that insolvency to pay a damage award may constitute irreparable harm even though economic harm is generally not considered to qualify." *Friendship Edison Pub. Charter Sch. Collegiate Campus v. Nesbitt*, 704 F. Supp. 2d 50, 52 (D.D.C. 2010); *Foltz v. U.S. News and World Kept., Inc.*, 613 F. Supp. 634, 643 (D.D.C. 1985) (concluding that the unavailability of assets to pay a damage award would irreparably injure plaintiffs).

Additionally, it is well-settled that consumer confusion and injury to business goodwill constitute irreparable harm. *Robert Half Int'l Inc. v. Billingham*, 315 F. Supp. 3d 419, 433 (D.D.C. 2018). "[I]t is generally recognized that '[t]rademark infringement by its very nature causes irreparable injury.'" *Capitol Educ. Support*, 589 F. Supp. 2d at 30; *see also Hanley-Wood LLC v. Hanley Wood LLC*, 783 F. Supp. 2d 147, 151 (D.D.C. 2011) (granting preliminary injunction after noting "[g]enerally, trademark infringement, by its very nature, carries a presumption of harm"); *AARP v. Sycle*, 991 F. Supp. 2d 224, 230 (D.D.C. 2013) (granting permanent injunction based on the presumption of harm in trademark infringement cases); *Delta Sigma Theta Sorority, Inc. v. Allen Prof'l Graphics Grp., LLC*, 212 F. Supp. 3d 116, 120 (D.D.C. 2014) (granting preliminary injunction and noting District of Columbia courts have repeatedly recognized that trademark

infringement by its very nature, causes irreparable injury"); *Malarkey-Taylor Assocs., Inc. v. Cellular Telecomms. Indus. Ass'n*, 929 F. Supp. 473, 478 (D.D.C. 1996) (finding "irreparable injury to the goodwill and reputation associated with [] trademark" that "could lead to dilution of the distinctiveness of the WirelessNOW trademark and loss of control over its reputation" which cannot be compensated in monetary damages).

Here, the Star Blizzard Defendants tarnish Plaintiffs' valuable trademarks, branding, reputation, and goodwill, injuring Plaintiffs' reputation and customer goodwill, creating confusion as to the source of the Star Blizzard Defendants' spear phishing and cybercrimes, and damaging the reputation of and confidence in Plaintiffs' services. These injuries are sufficient in and of themselves to constitute irreparable

1. Irreparable Harm to Microsoft

To carry out its criminal operation, the Star Blizzard Defendants use Microsoft based software and services. Ensz Decl. ¶¶ 29-32. This is done intentionally to improperly leverage Microsoft's brandings, trademarks, and reputation and to deceive victims into believing that the Star Blizzard malicious attacks are associated or endorsed by Microsoft. *Id.* ¶ 47. If a customer mistakenly believes that Microsoft endorses the cybercriminal behavior of the Star Blizzard Defendants, Microsoft's reputation and goodwill is harmed beyond repair—indeed, in such circumstances the customer may be lost forever. *Id.* ¶¶ 47-51.

2. Irreparable Harm to NGO-ISAC and Member Organization

NGO-ISAC and its member organizations are irreparably harmed when the Star Blizzard Defendants impersonate the NGO-ISAC member organization. Ensz Decl. ¶ 52; Gottesman Decl. ¶¶ 15-16. When the Star Blizzard Defendants impersonate NGO-ISAC member organizations this harms the targeted victim's career and reputation, as well as the reputation of the NGO the victim

is associated with and the overall efficacy of the NGO's policy work objective. Ensz Decl. ¶¶ 49-50. Carnegie Corporation's reputation was harmed when its trusted and well-known grant program was impersonated by the Star Blizzard Defendants to trick potential grantees into believing that the spear phishing emails were actually coming from Carnegie Corporation. Sherman Decl. ¶¶ 9-11. The harm caused by the Star Blizzard Defendants are irreparable because its impersonation and spear phishing campaign has eroded trust within the community. Gottesman Decl. ¶ 17.

C. The Balance of Equities Strongly Favor Injunctive Relief.

This Court has recognized that "[t]he balance of harms cannot favor a defendant whose injury results from the knowing infringement on the plaintiff's trademark." *Allen Prof'l*, 212 F. Supp. 3d at 120 (finding defendants will not suffer substantial harm from preliminary injunction where injunction would only prevent defendants from using plaintiff's marks, which defendants are not authorized to do). On one side of the scales of equity rests the harm to Plaintiffs, their customers and member organizations, and the public caused by the Star Blizzard Defendants, while on the other side the Star Blizzard Defendants can claim no legally cognizable harm because an injunction would only require them to cease illegal activities. *Youngstown Sheet & Tube Co. v. Sawyer*, 103 F. Supp. 569, 576, 62 Ohio Law Abs. 405 (D.D.C 1952) (balance of equities favored plaintiff where defendants were engaged in illegal acts).

D. The Public Interest Favors Injunctive Relief.

It is clear that an injunction would serve the public interest here. With every day that passes, the Star Blizzard Defendants engage in more spear phishing, have infiltrated more computer networks, and have stolen more sensitive information from their innocent victims. Moreover, the public interest is clearly served by enforcing statutes designed to protect the public, such as the Lanham Act, CFAA, and ECPA. *McVeigh v. Cohen*, 983 F. Supp. 215, 221 (D.D.C.

1998) (granting preliminary injunction in case involving ECPA and noting "[w]ith literally the entire world on the worldwide web, enforcement of the ECPA is of great concern to those who bare the most personal information about their lives in private accounts through the Internet'); *Estate of Coll-Monge v. Inner Peace Movement*, 524 F.3d 1341, 1350 (D.C. Cir. 2008) (finding public interest was served by TRO to prevent people from being deceived by defendant impersonating plaintiff); *Crime Control, Inc. v. Crime Control, Inc.*, 624 F. Supp. 579, 582 (D.D.C. 1984) (granting preliminary injunction because "the public has a right not to be deceived or confused"); *Hanley-Wood*, 783 F. Supp. 2d at 151 (granting permanent injunction because "the public interest favors protecting against further violation of federal copyright and trademark laws").

Numerous courts that have addressed requests for injunctive relief targeted at disabling malicious command and control infrastructures have granted such relief. *Microsoft Corp. v. John Does 1-2*, Case No. 1:19-cv-00716 (2019 D.D.C) (Jackson, J.) (*ex parte* TRO and preliminary injunction to dismantle Phosphorus cybercriminal operation); *Microsoft Corp. v. Peng Yong et al.*, Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.) (*Ex Parte* TRO to dismantle botnet command and control servers); *Microsoft Corp. v. Piatti, et al.,* Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.) (*Ex Parte* TRO and preliminary injunction to dismantle botnet command and control servers); *Microsoft Corp. v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va. 2010) (Brinkema, J.) (same); *Microsoft Corp. v. John Does 1-11*, Case No. 2:11-cv-00222 (W.D. Wash. 2011) (Robart, J.) (same); *Microsoft Corp. et al. v. John Does 1-39 et al.*, Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.) (same); *FTC v. Pricewert LLC et al.*, Case No. 09-2407 (N.D. Cal. 2009) (Whyte, J.) (*Ex Parte* TRO and preliminary injunction disconnecting service to botnet hosting company). The same result is warranted here.

In each of the foregoing cases, asserting the same claims as this case, the courts granted as a remedy the transfer of malicious domains to Microsoft's control, and away from the control of the Star Blizzard Defendants. Such relief is not prohibited by any statute or rule of law, is appropriate and necessary, and within the Court's broad equitable authority to craft remedies to prevent irreparable harm. The federal courts have very broad, inherent equitable authority to craft injunctions for any civil violation of law – including violations of CFAA, ECPA or any other civil cause of action. *See e.g.*, *Weinberger v. Romero-Barcelo*, 456 U.S. 305, 313 (1982) ("Unless a statute in so many words, or by a necessary and inescapable inference, restricts the court's jurisdiction in equity, the full scope of that jurisdiction is to be recognized and applied."); *Federal Marine Terminals, Inc. v. Burnside Shipping Co.*, 394 U.S. 404, 412 (1969) ("the legislative grant of a new right does not ordinarily cut off or preclude other nonstatutory rights in the absence of clear language to that effect").

There is nothing within the CFAA, ECPA or the Lanham Act, that limits the federal court's equitable authority for violation of CFAA. For example, the CFAA, at 18 U.S.C. 1030(g), contemplates broadly that "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." This evinces a Congressional intent to afford broad remedies and, clearly, the federal courts have taken that view in prior cybercrime matters brought by Microsoft. Disablement of the Star Blizzard Defendants' malicious command and control infrastructure is well within the Court's broad equitable authority to craft such remedies.

V. THE ALL WRITS ACT AUTHORIZES THE COURT TO DIRECT THIRD PARTIES TO PERFORM THE NECESSARY ACTS TO AVOID FRUSTRATION OF THE REQUESTED RELIEF.

Plaintiffs' Proposed Order directs that the third-party domain registrars and registries

whose infrastructure the Star Blizzard Defendants rely on to operate Star Blizzard's command and control infrastructure reasonably cooperate to effectuate the order. Critically, these third parties are the primary entities within the United States that can effectively disable command and control Infrastructure, and thus their cooperation is necessary.

Plaintiffs request this relief under the All Writs Act. The All Writes Act provides that a court may issue all writs necessary or appropriate for the administration of justice. 28 U.S.C. § 1651(a). The Supreme Court has recognized that the All Writs Act can extend to third-parties necessary to effect the implementation of a court order. *United States v. New York Tel. Co.*, 434 U.S. 159, 174 (1977) (All Writs Act extends to third parties who "are in a position to frustrate the implementation of a court order or the proper administration of justice" and holding that order applied to third-party telephone company to assist in implementation of a pen register warrant was authorized under the All Writs Act); *Sarnecka-Crouch v. Billington*, 2012 WL 3060165, at *2 (D.D.C. July 26, 2012) (ordering Commissioner of the Social Security Administration to provide the Library of Congress with all documents pertaining to plaintiffs Social Security benefits account for the period 2005-2009); *Evans v. Williams*, 1999 WL 1212884, at *3 (D.D.C. Aug. 20, 1999) (finding no other effective means exists to address specifically the continuing unwillingness of the Superior Court to provide access to the information required by District of Columbia Court other than using power under the All Writs Act).

Requiring these third parties to reasonably assist in the execution of this order will not offend Due Process as the Proposed Order (1) requires only minimal assistance from the third parties in executing the order (transferring domain ownership, which is an act that registrars and registries take in the ordinary course of their operations), (2) requires that it be implemented with the least degree of interference with the normal operation of third parties, (3) does not deprive the

third parties of any tangible or significant property interests and (4) requires Plaintiffs to compensate the third parties for the assistance rendered. If, in the implementation of the Proposed Order, any third party wishes to bring an issue to the attention of the Court, Plaintiffs will bring it immediately. The third parties will have an opportunity to be heard at the preliminary injunction hearing, which must occur shortly after the execution of the Proposed Order. Fed. R. Civ. P. 65(b)(2). The directions to third parties in the Proposed Order are thus narrow, satisfy Due Process, and are necessary to effectuate the requested relief to ensure that the relief is not rendered fruitless.

VI. AN *EX PARTE* TRO IS THE ONLY EFFECTIVE MEANS OF RELIEF, AND ALTERNATIVE SERVICE IS WARRANTED UNDER THE CIRCUMSTANCES.

The TRO that Plaintiffs request must issue *ex parte* for the relief to be effective at all because of the extraordinary factual circumstances here—namely, the Star Blizzard Defendants' technical sophistication and ability to move their malicious infrastructure if given advance notice of Plaintiffs' request for injunctive relief. Rule 65 of the Federal Rules of Civil Procedure permits an *ex parte* TRO where the moving party sets forth facts that show an immediate and irreparable injury and why notice should not be required. Fed. R. Civ. P. 65(b)(1); *see Granny Goose Foods, Inc. V. Brotherhood of Teamsters & Auto Truck Drivers, Local No. 70,* 415 U.S. 423, 439 (1974) ("*Ex parte* temporary restraining orders are no doubt necessary in certain circumstances....").

If notice is given prior to issuance of a TRO, it is likely that the Star Blizzard Defendants will be able to quickly mount an alternate command and control structure and direct the vast majority of the infiltrated computers to begin to communicate through that alternate structure before the TRO can have any remedial effects. Ensz Decl. ¶¶ 57-59. Thus, providing notice of the requested TRO will undoubtedly facilitate efforts by the cybercriminals to continue to operate Star Blizzard. *Id.* It is well established that *ex parte* relief is appropriate under circumstances such as the instant case, where notice would render the requested relief ineffective. *See, e.g.*,

AllscriptsMisys, LLC v. Am. Dig. Networks, LLC, 2010 U.S. Dist. LEXIS 4450, at *2 (D. Md. Jan. 20, 2010) (granting an *ex parte* TRO where "Defendant may dissipate the funds and/or take action to render it difficult to recover funds"); *AT&T Broadband v. Tech Commc'ns, Inc*., 381 F.3d 1309, 1319-1320 (11th Cir. 2004) (affirming *ex parte* search and seizure order to seize contraband technical equipment, given evidence that in the past defendants and persons similarly situated had secreted evidence once notice given); *Little Tor Auto Ctr. v. Exxon Co., U.S.A.*, 822 F. Supp. 141, 143 (S.D.N.Y. 1993) (*ex parte* TRO appropriate where contraband "may be destroyed as soon as notice is given"); *Crosby v. Petromed, Inc.*, 2009 WL 2432322, at *2 (E.D. Wash. Aug. 6, 2009) (granting *ex parte* TRO as "notice to Defendants of this TRO request could result in further injury or damage to Plaintiffs...."). Similarly, in *FTC v. Pricewert LLC*, the district court issued an *ex parte* TRO suspending Internet connectivity of a company enabling botnet activity and other illegal computer-related conduct on the basis that "Defendant is likely to relocate the harmful and malicious code it hosts and/or warn its criminal clientele of this action if informed of the [plaintiff's] action." *See FTC v. Pricewert LLC et al.*, Case No. 09-2407 (N.D. Cal.) (Whyte, J.) at 3.

Here, there is specific evidence that the Star Blizzard Defendants will attempt to move the infrastructure if given notice, as the Star Blizzard Defendants have persistently changed infrastructure once it becomes known to the security community, in order to stay ahead of cybersecurity counter-measures. Ensz Decl. ¶¶ 60-61. Accordingly, granting *ex parte* relief without first providing notice is appropriate. Indeed, district courts have previously granted similar relief in cases brought by Microsoft to halt similarly situated cybercriminal operations.

To ensure due process, immediately upon entry of the requested *ex parte* TRO, Plaintiffs will undertake extraordinary efforts to effect formal and informal notice of the preliminary

injunction hearing to the Star Blizzard Defendants and to serve the complaint.

Plaintiffs Will Provide Notice to the Star Blizzard Defendants by Personal Delivery: Plaintiffs have identified domains from which the Star Blizzard Defendants' command and control operates, and, pursuant to the TRO, will obtain from the domain registrars/registries any and all physical addresses of the Star Blizzard Defendants, to the extent those are available or not fictitious. Pursuant to Rules 4(e)(2)(A) and 4(f)(3), Plaintiffs plan to effect formal notice of the preliminary injunction hearing and service of the complaint by personal delivery of the summons, Plaintiffs' Complaint, the instant motion and supporting documents, and any Order issued by this Court to such addresses in the United States. Poston Decl. ¶ 13.

Plaintiffs Will Provide Notice to the Star Blizzard Defendants by Email, Facsimile, and Mail: Plaintiffs have identified email addresses, mailing addresses and/or facsimile numbers provided by the Star Blizzard Defendants, and will further identify such contact information pursuant to the terms of the requested TRO. Poston Decl. ¶ 10. Plaintiffs will provide notice of the preliminary injunction hearing and will effectuate service of the Complaint by immediately sending the same pleadings described above to the email addresses, facsimile numbers and mailing addresses that the Star Blizzard Defendants provided to the registrars and registries. *Id.*. When the Star Blizzard Defendants registered for domain names, they agreed not to engage in abuse such as that at issue in this case and agreed that notice of disputes regarding hosting could be provided to them by sending complaints to the email, facsimile and mail addresses provide by them. Poston Decl. ¶¶ 15-28.

Plaintiffs Will Provide Notice to the Star Blizzard Defendants by Publication: Plaintiffs will notify the Star Blizzard Defendants of the preliminary injunction hearing and the Complaint against their misconduct by publishing the materials on a centrally located, publicly

accessible source on the Internet. Poston Decl. ¶ 11.

Plaintiffs Will Provide Notice to the Star Blizzard Defendants by Personal Delivery and Treaty if Possible: If valid physical addresses of the Star Blizzard John Doe Defendants can be identified, Plaintiffs will notify the Star Blizzard Defendants and serve process upon them by personal delivery or through the Hague Convention on service of process or similar treaty-based means. Poston Decl. ¶ 14.

Notice and service by the foregoing means satisfy due process; are appropriate, sufficient, and reasonable to apprise the Star Blizzard Defendants of this action; and are necessary under the circumstances. Plaintiffs hereby formally request that the Court approve and order the alternative means of service discussed above. First, legal notice and service by email, facsimile, mail, and publication satisfies due process as these means are reasonably calculated, in light of the circumstances, to apprise the interested parties of the TRO, the preliminary injunction hearing, and the lawsuit. *See Mullane v. Cent. Hanover Bank & Tr. Co.*, 339 U.S. 306, 314 (1950). Such methods are also authorized under Federal Rule of Civil Procedure 4(f)(3), which allows a party to serve defendants by means not prohibited by international agreement. The methods of notice and service proposed by Plaintiffs have been approved in other cases involving international defendants attempting to evade authorities. *Rio Properties, Inc. v. Rio Int'l. Interlink*, 284 F.3d 1007, 1014- 15 (9th Cir. 2002) (authorizing service by email upon an international defendant); *AllscriptsMisys*, 2010 U.S. Dist. LEXIS 4450, at *3 (granting *ex parte* TRO and order prompting "notice of this Order and Temporary Restraining Order as can be effected by telephone, electronic means, mail or delivery services."); *Bazarian Int'l Fin. Assocs., L.L.C. v. Desarrollos Aerohotelco, C.A.*, 168 F. Supp. 3d 1, 13-16 (D.D.C. 2016) (noting Rule 4(f) is "concerned with providing a method of service that is reasonably calculated to 'notif[y] a defendant of the commencement of

an action against him" and upholding service through U.S. counsel). Such service is particularly warranted in cases such as this involving Internet-based misconduct, carried out by international defendants, causing immediate, irreparable harm. *Rio Properties*, 284 F.3d at 1018. Notably, *Rio Properties* , a Ninth Circuit case, has been followed by District of Columbia courts. *See Juniper Networks, Inc. v. Bahattab*, 2008 WL 250584, at *2 (D.D.C. Jan. 30, 2008) (finding "service of process via electronic mail and facsimile is appropriate and may be authorized by the Court under Rule 4(f)(3) of the Federal Rules of Civil Procedure").

In this case, the e-mail addresses provided by the Star Blizzard Defendants to the domain registrars, in the course of obtaining services that support the Star Blizzard operation are likely to be the most accurate and viable contact information and means of notice and service. Ensz Decl. ¶¶ 36, 39, 41. Moreover, the Star Blizzard Defendants will expect notice regarding their use of the domain registrars' services to operate Star Blizzard by those means, as the Star Blizzard Defendants agreed to such in their agreements. *See Nat'l Equip. Rental, Ltd. v. Szukhent*, 375 U.S. 311,315-16 (1964) ("And it is settled ... that parties to a contract may agree in advance to submit to the jurisdiction of a given court, to permit notice to be served by the opposing party, or even to waive notice altogether."). For these reasons, notice and service by e-mail and publication are warranted and necessary here.[6]

Thus, Plaintiffs request that the Court order that the means of notice of the preliminary injunction hearing and service of the complaint set forth herein meet Fed. R. Civ. Pro. 4(f)(3)

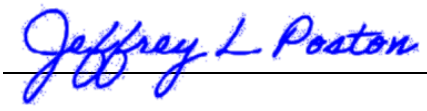
[6] Additionally, if the physical addressees provided by the Star Blizzard Defendants to domain registrars turn out to be false and their whereabouts are unknown, the Hague Convention will not apply in any event and alternative means ofservice, such as email and publication, would be appropriate for that reason as well. *BP Prod. N. Am., Inc. v. Dagra*, 236 F.R.D. 270, 271 (E.D. Va. 2006) ("The Hague Convention does not apply in cases where the address of the foreign party to be served is unknown.").

satisfy due process and are reasonably calculated to notify the Star Blizzard Defendants of this action.

VII. CONCLUSION

For the reasons set forth herein, Plaintiffs respectfully request that this Court grant the instant motion for a TRO and issue an order to show cause regarding a preliminary injunction.

Dated: September 24, 2024



Jeffrey L. Poston (DC Bar No. 426178)
JPoston@crowell.com
Garylene Ana Joji D. Javier (*pro hac vice* pending)
GJavier@crowell.com
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington, DC 20004

Anna Z. Saber (*pro hac vice* pending)
ASaber@crowell.com
CROWELL & MORING LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111

Attorneys for Plaintiffs Microsoft Corporation and NGO-ISAC

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Microsoft Corporation, a Washington State Corporation, NGO-ISAC, a New York State Non-Profit Organization, Plaintiffs, v. John Does 1-2, Controlling A Computer Network and Thereby Injuring Plaintiff and Its Customers, Defendants.	Civil Action No. **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5.1**

DECLARATION OF SEAN ENSZ IN SUPPORT OF APPLICATION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, Sean Ensz, declare as follows:

1. I am a Principal Investigator in Microsoft Corporation's Digital Crimes Unit ("DCU"). I make this declaration in support of Microsoft's Application for an Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause Re: Preliminary Injunction. I make this declaration of my own personal knowledge or on information and belief where indicated. If called as a witness, I could and would testify competently to the truth of the matters set forth herein.

2. I have been employed by Microsoft since July 2018. In my role at Microsoft, I work as a Digital Crimes Unit Principal Investigator, and I investigate significant transnational cybercrime and nation state incidents and develop threat intelligence to disrupt malicious cyber operations. Prior to joining Microsoft in 2018, I served as the Information Assurance Manager at Devon Energy and spent ten years in information technology at the University of Oklahoma conducting and managing forensic investigations and incident response teams. A true and correct

copy of the current version of my curricula vitae is attached to this declaration as **Exhibit 1**.

3. My declaration concerns the investigation into a Russia-based cybercriminal organization comprised of unknown individuals collectively known as "Star Blizzard" that is systematically and persistently engaging in cyberattacks that include developing infrastructure and capabilities to conduct spear phishing attacks to facilitate cybercrime, as detailed below. I discuss Star Blizzard's victim targeting methodology, techniques, tools used to execute their techniques, and harm to Microsoft, its customers, and the public.

I. CYBERCRIME AT ISSUE: SPEAR PHISHING CAMPAIGNS

4. I, along with other Microsoft investigators, investigate cybercrime campaigns like spear phishing, that are perpetrated by threat actors that target Microsoft and its customers. In this function, Microsoft identified and investigated Star Blizzard's spear phishing campaign.

5. As a Principal Investigator experienced in investigating cybercrimes, I have observed threat actors often use a social engineering tactic called phishing. Phishing attacks use deceptive emails tailored to use deceptive language to elicit fear or urgency by the recipient, to trick them into interacting with the email, such as clicking on a link or opening a file. The intent of phishing typically includes installing malware, stealing someone's account credentials, or to reveal personal information (such as credit card numbers, bank information, or passwords). These emails often include links to websites that appear legitimate but are in fact, controlled by threat actors as part of their operation to steal information. Files attached in phishing emails may be infected with malicious computer software ("malware") or include hyperlinks to threat actor-controlled websites. Threat actors use this tactic on a grand scale called campaigns, which are repeated, persistent attempts to target multiple victims to achieve their objective.

6. A spear phishing campaign is a type of attack where phishing emails are tailored to

a specific group, organization, or person, to increase the likelihood of stealing their target's credentials and data by convincing them of the email's legitimacy. This often includes: (i) using local language for the subject, body, and sender's name to make it harder for users to identify email as a spear phishing attempt; (ii) email topics that correspond to the recipient's responsibilities in the organization, e.g., sending academic or policy papers; or (iii) using compromised or impersonated email accounts to send spear phishing emails that appear legitimate and from a known sender.

7. Threat actors, particularly foreign criminal organizations or groups associated with foreign governments, use spear phishing to engage in information gathering, online influence, and espionage.

II. STAR BLIZZARD DEFENDANTS

Foreign Cybercriminals

8. My declaration concerns the investigation into the persistent spear phishing campaigns by the Star Blizzard Defendants – hostile cybercriminals believed to be operating from Russia. The identities of the cybercriminals behind the activities addressed in this declaration are uncertain and are collectively identified by the threat actor name that Microsoft has assigned to this group: "Star Blizzard." The Star Blizzard Defendants are formerly known as SEABORGIUM and also known in the cybersecurity community as the Callisto Group, COLDRIVER, and BlueCharlie.

Motivation and Targeted Victims

9. The Star Blizzard Defendants' primary objectives are information gathering, cyber influence, and cybercrime.

10. Since the beginning of 2022, Microsoft has observed the Star Blizzard Defendants' campaigns target over 30 organizations, in addition to personal accounts of people of interest. The Star Blizzard Defendants primarily target NATO countries, particularly the United States and the United Kingdom, and other countries in the Baltics, the Nordics, and Eastern Europe. Such targeting has included the government sector of Ukraine in the months leading up to the invasion by Russia, and organizations involved in supporting roles for the war in Ukraine. Despite some targeting of these organizations, Microsoft assesses that Ukraine is likely not a primary focus for this actor (as the Star Blizzard Defendants have also targets organization and individuals that work to oppose the Russian government and are adverse to Russia's interests or global and domestic policy beyond its invasion of Ukraine); however, it is most likely a reactive focus area for the actor and one of many diverse targets.

11. Within the target countries like the U.S., the Star Blizzard Defendants primarily focuses cyber operations on individuals working in defense and intelligence consulting companies, non-governmental organizations (NGOs) and intergovernmental organizations (IGOs), governmental policy think tanks, and higher education. The Star Blizzard Defendants have a high interest in targeting personal email accounts as well, with 30% of Microsoft's victim notifications related to the Star Blizzard Defendants' activities being delivered to Microsoft consumer email accounts. The Star Blizzard Defendants have also been observed targeting former intelligence officials, experts in Russian affairs, and Russian citizens abroad in the U.S.

12. Since 2023, Microsoft has observed the Star Blizzard Defendants' campaigns continue to target NGOs, think tanks, government employees, and personal accounts belonging to current and former military and intelligence officials and policy advisors. The individuals targeted by these attacks predominately reside in the U.S., in and around the Washington, DC area.

13. The identified spear phishing campaigns are methodically crafted using email addresses that appear legitimate by representing a person known to the target using subject lines and imbedded or attached documents to lure the recipient into opening. In some cases, previously compromised accounts, known to the spear phishing target, are directly used by the Defendants to increase the likelihood of success.

14. Microsoft has identified 82 customers that have been targeted by the Star Blizzard Defendants since January 2023, at a rate of about once per week. This rate indicates the level of care used by Star Blizzard to identify targets, craft custom spear phishing emails, and develop the infrastructure needed to facilitate credential theft, and cull the target's mailbox sensitive documents and known contacts to develop additional targets if the target is compromised.

III. INVESTIGATING THE ATTACK CHAIN

15. Microsoft's investigation has established the Defendants have developed the following steps to successfully spear phish targets, Defendants: i) registers deceptive domains, ii) configures a AiTM web proxy to host deceptive domain, iii) sends phishing email using the deceptive domain deliver malicious content through a link to Microsoft's personal cloud storage platform, OneDrive, or by adding a malicious URL in the body of an email or PDF file attachment, iv) steals their credentials, and v) culls mailboxes to exfiltrate sensitive data and contacts. The Star Blizzard Defendants have successfully compromised organizations and people of interest in persistent spear phishing campaigns, infrequently changing their procedures and tactics. **Figure 1** is a visual representation of the Star Blizzard attack chain.

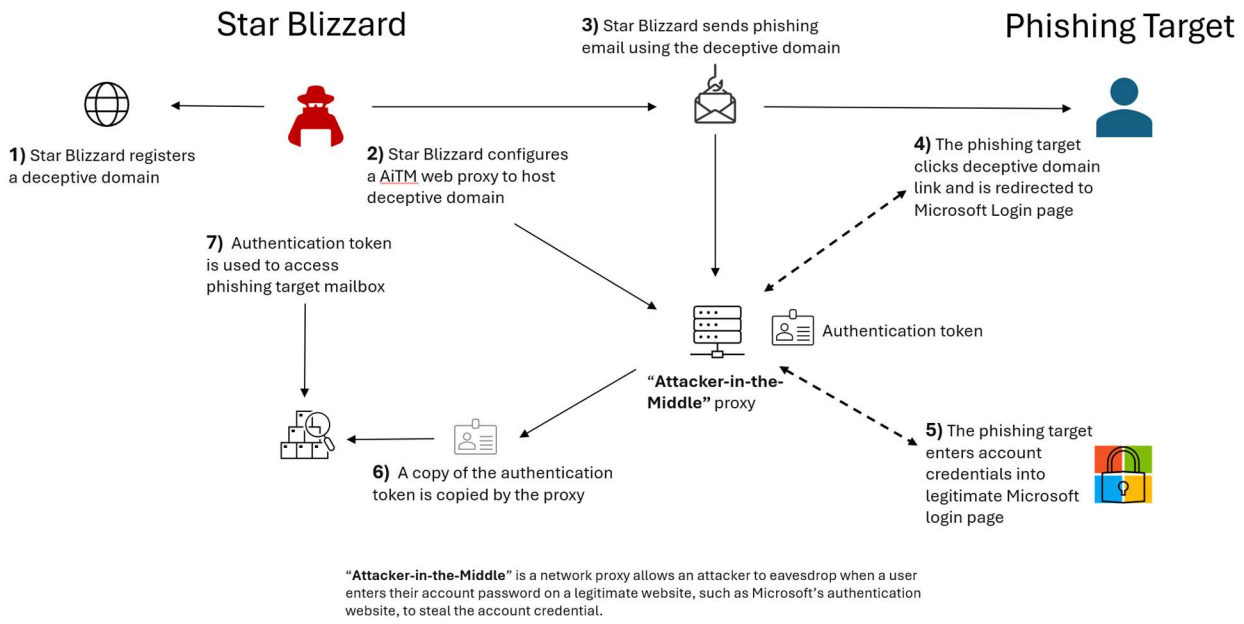


Figure 1

Attack Step 1: Impersonation and Establishing Contact

16. Before starting a campaign, the Star Blizzard Defendants often conducts reconnaissance of target individuals, with a focus on identifying legitimate contacts in the target's social network or sphere of influence.

17. Based on some of the impersonation and targeting observed, we suspect that the Star Blizzard Defendants use social media platforms, personal directories, and general open-source intelligence (OSINT) to supplement their reconnaissance efforts. The Star Blizzard Defendants often use their target's social networks through contact impersonation, rapport building, and additional spear phishing to deepen their intrusion.

18. In coordination with Microsoft's Microsoft Threat Intelligence Center (MSTIC), and partnership with LinkedIn, Microsoft observed fraudulent profiles attributed to the Star Blizzard Defendants being used sporadically for conducting reconnaissance of employees from

specific organizations of interest. **Figure 2** below is an example profile used by the Star Blizzard Defendants to conduct industry-specific reconnaissance. In accordance with their policies, LinkedIn terminated any account (including the one shown below) identified as conducting inauthentic or fraudulent behavior.

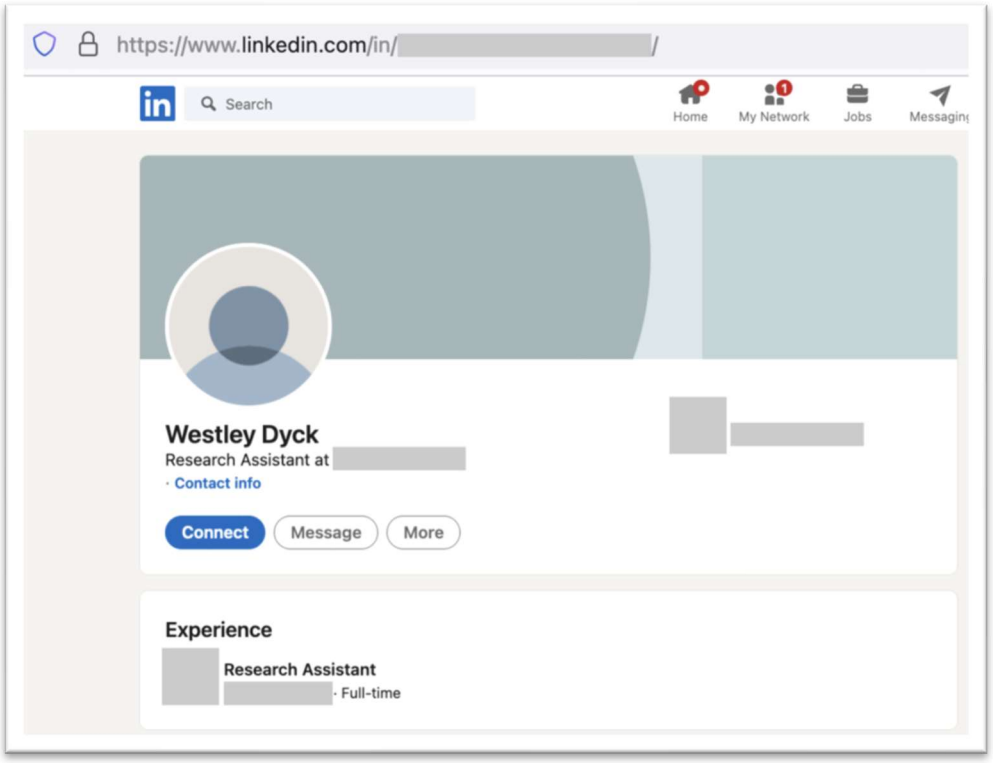


Figure 2[1]

19. Defendants also register new email accounts at various consumer email providers, with the email address or alias configured to match legitimate aliases or names of impersonated

[1] Identifying information contained within this figure and others figures included in this declaration have been redacted for privacy of the targets and victims of the Star Blizzard Defendants.

individuals. For example, attached to this declaration is **Exhibit 2**[2] which are true and correct copies of threat research reports by the Cybersecurity and Infrastructure Security Agency (CISA) discussing the Star Blizzard Defendants' various tactics and techniques. It outlines several tactics, including the registration of consumer email accounts matching the names of individuals they are impersonating to conduct spear-phishing activity.

20. While the creation of new consumer accounts is common, we have also observed Defendants returning to and reusing historical accounts that match the industry of the ultimate target. In one case, we observed the Star Blizzard Defendants returning to an account it had not used in a year, indicating potential tracking and reusing of accounts if relevant to targets' industry.

21. After registering new accounts, the Star Blizzard Defendants proceed to establish contact with their target. In cases of personal or consumer targeting, Microsoft has mostly observed the actor starting the conversation with a benign email message, typically exchanging pleasantries before referencing a non-existent attachment while highlighting a topic of interest to the target. It is likely that this additional step helps the actor establish rapport and avoid suspicion, resulting in further interaction. If the target replies, the Star Blizzard Defendants proceed to send a weaponized email. **Figure 3** below is an example email showing the multi-email approach and rapport building frequently used by Defendants.

[2] Russian FSB Cyber Actor Star Blizzard Continues Worldwide Spear-phishing Campaigns, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-341a.

Figure 3

22. Microsoft has documented several cases where the Star Blizzard Defendants focus on a more organizational approach to spear phishing. In these cases, they use an authoritative approach in their social engineering (psychological manipulation to trick users into making security mistakes or giving away sensitive information) and typically goes to directly sending malicious content. **Figure 4** is an example of a spear phishing email where a Star Blizzard Defendant impersonates the lead of an organization and emails select members of the organization with a cybersecurity themed lure.

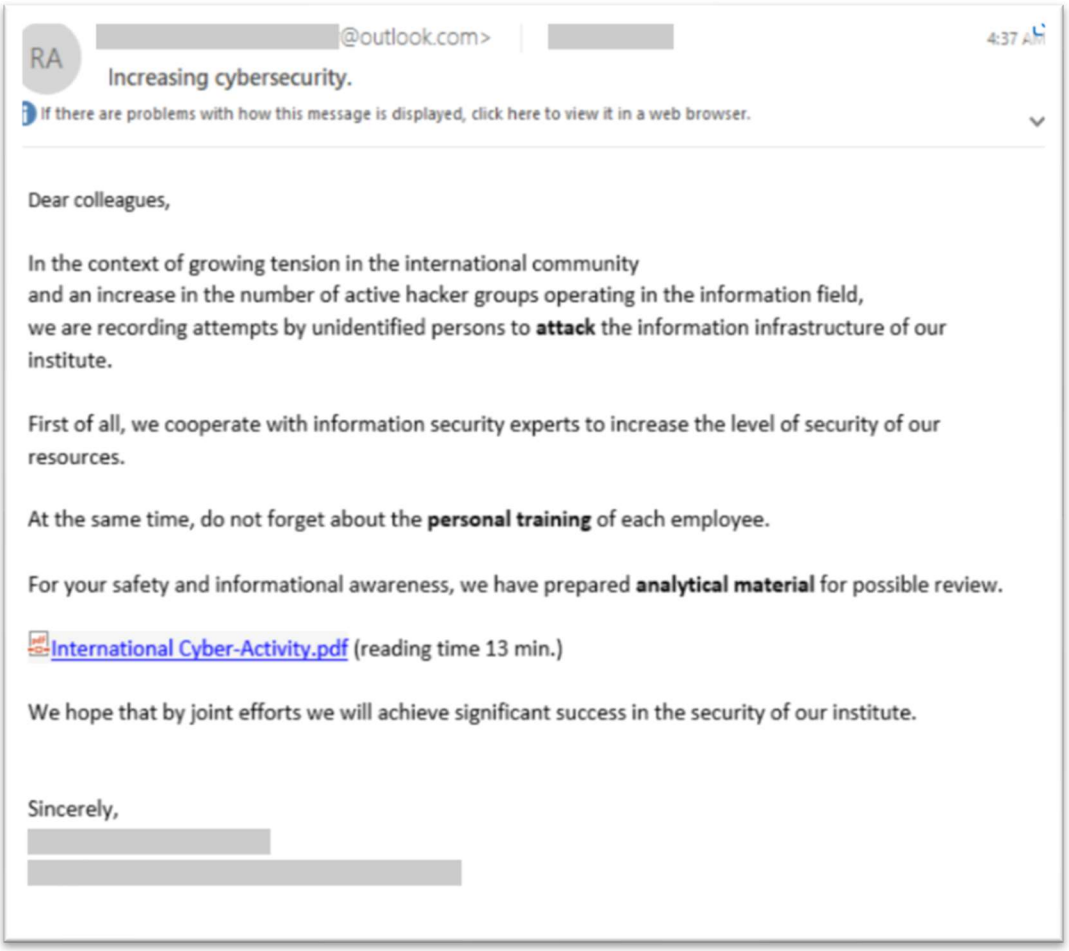


Figure 4

23. These examples serve to demonstrate the actors' capability to be dynamic and to adapt their social engineering approach to gain the trust of their victims.

Attack Step 2: Deliver Malicious Content

24. Microsoft investigation into the Star Blizzard Defendants' activities identified several variations in the way that the Star Blizzard Defendants delivers a link that directs targets to their credential stealing infrastructure.

Delivery Method #1 - Malicious Uniform Resource Locator (URL) in an Email

25. In the simplest case, the Star Blizzard Defendants directly add a URL to the body of their phishing email. A URL (Uniform Resource Locator) is a unique identifier used to locate a resource on the Internet. It is also referred to as a web address.

26. Occasionally, Defendants use URL shorteners which shortens the link to sometimes hide the website domain and make it look random. The Star Blizzard Defendants also use open redirects to obfuscate their web address from the security tools. Open redirect is a cyber exploit that occurs when a website redirects a user to a different, often malicious URL. This redirection is typically achieved through a crafted hyperlink supplied by Defendants, exploiting the trust users have in the genuine website.

27. The email varies between fake personal correspondence with a hyperlinked text and fake file sharing emails that imitate a range of platforms. **Figure 5** is an example of a follow-up email impersonating a OneDrive share. The link embedded takes the user to Defendant controlled infrastructure.

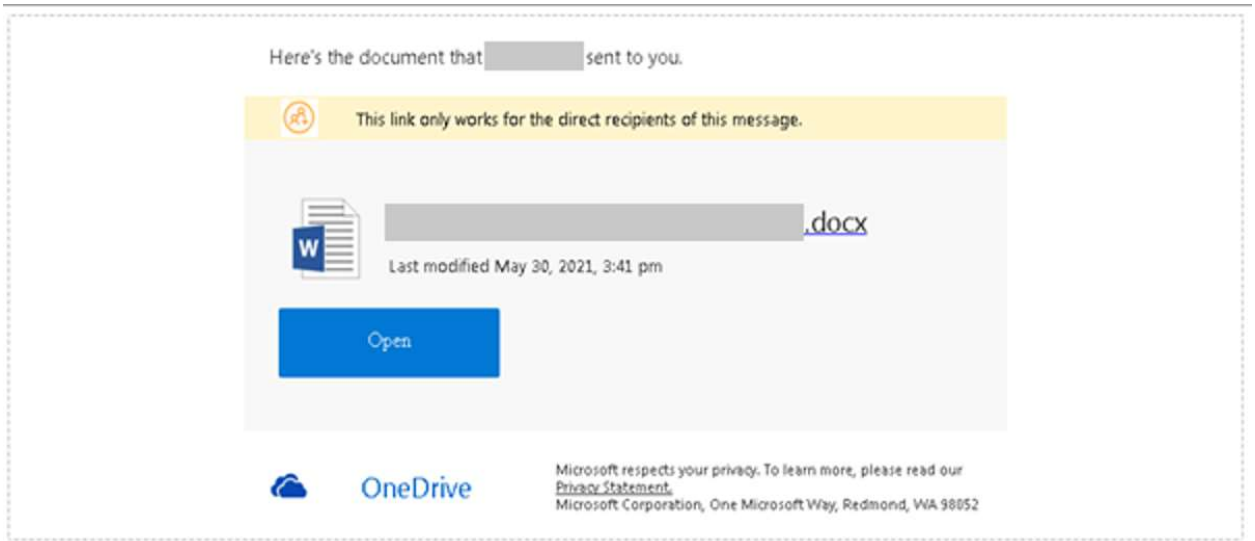


Figure 5

Delivery Method #2 - PDF File Attachment Contains Malicious URL

28. Microsoft has observed an increase in the use of attachments in the Star Blizzard Defendants' spear phishing campaigns. These attachments typically imitate a file or document hosting service, including OneDrive, and request the user to open the document by clicking a button. **Figure 6** and **Figure 7** are examples of a spear phishing email using the war in Ukraine as a ruse with the Star Blizzard Defendants directly attaching a PDF file to the email. Once a recipient downloads and attempts to open the attached, PDF file, the file appears to be a failed preview, redirecting the users to click a link which takes the user to Star Blizzard-controlled infrastructure.

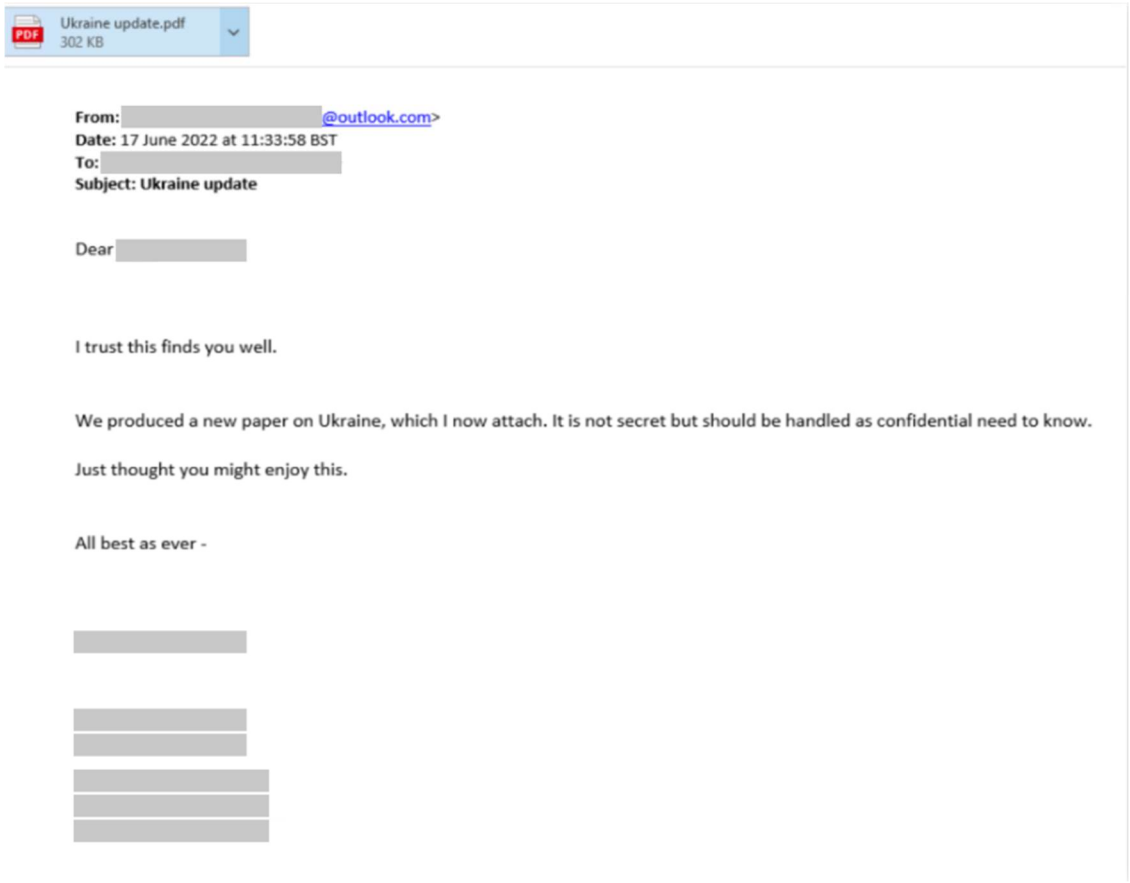


Figure 6

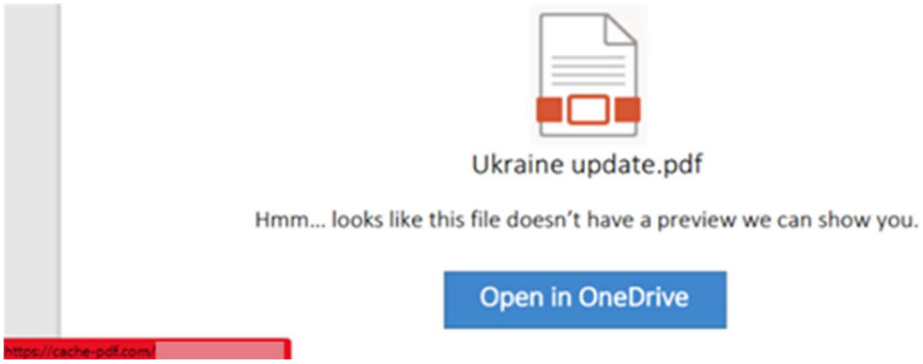


Figure 7

Delivery Method #3 - OneDrive Link to PDF File Containing a Malicious URL

29. The Star Blizzard Defendants abuse OneDrive or other file sharing platform to host PDF files that contain a link to the malicious URL. This activity does not represent any security issues or vulnerabilities on the OneDrive platform. The Star Blizzard Defendants include a OneDrive link in the body of the email that when clicked directs the user to a PDF file hosted within a Star Blizzard-controlled OneDrive account. As seen in the previous example, the victim is presented with what appears to be a failed preview message, enticing the target to click the link to be directed to the credential-stealing infrastructure. Occasionally, the Star Blizzard Defendants makes use of open redirects within the PDF file to further disguise their operational infrastructure. In the example below, Defendants use a Google URL for redirection. **Figure 8** is an example of a document hosted on OneDrive that uses a Google redirect link to send users to Star Blizzard-controlled infrastructure. **Figure 9** is an example of another file sharing platform, Proton Drive, also being impersonated by the Star Blizzard Defendants.

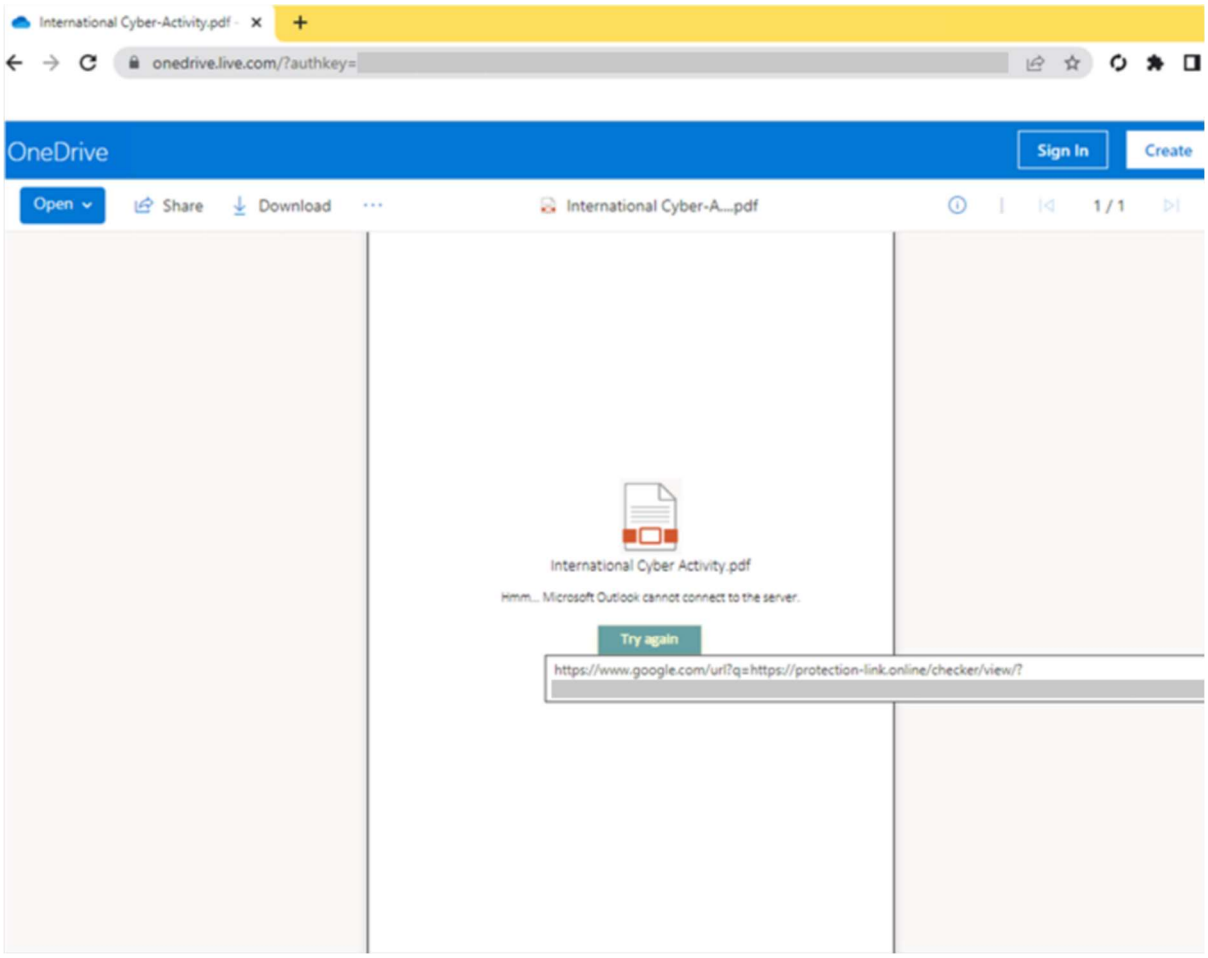

International Cyber-Activity.pdf
onedrive.live.com/?authkey=
OneDrive
Sign In
Create
Open
Share
Download
International Cyber-A....pdf
1 / 1
International Cyber Activity.pdf
Hmm... Microsoft Outlook cannot connect to the server.
Try again
https://www.google.com/url?q=https://protection-link.online/checker/view/?

Figure 8

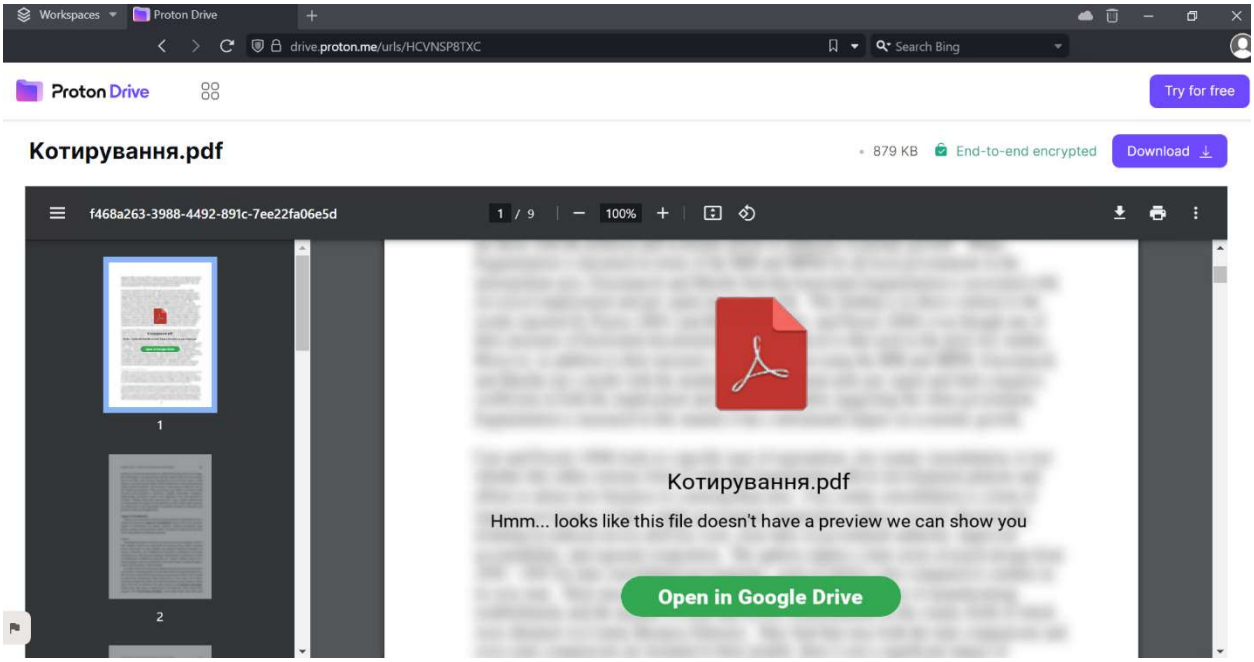


Figure 9

Attack Step 3: Capture Credentials and Exfiltrate Data

30. Based on Microsoft's investigations, regardless of the method of delivery, when the target clicks the URL, the target is directed to a Star Blizzard-controlled virtual server hosting a phishing proxy framework. A proxy or proxy server acts as a go-between a user and the Internet, offering privacy, access, and security. Threat actors exploit proxy servers by using it to hide their activities.

31. The Star Blizzard Defendants often use a malicious proxy framework Evilginx, which is an advanced phishing tool that act as "man-in-the-middle" attack. This type of attack intercepts network communications between a user's browser and a legitimate website, stealthily capturing login credentials and authentication cookies, even if the account uses two-factor authentication (2FA). This is what allows the Star Blizzard Defendants to re-access the target's account at later time without requiring the target to perform the similar activity of clicking on a controlled link and inputting in credentials). This process is depicted in **Figure 10.**

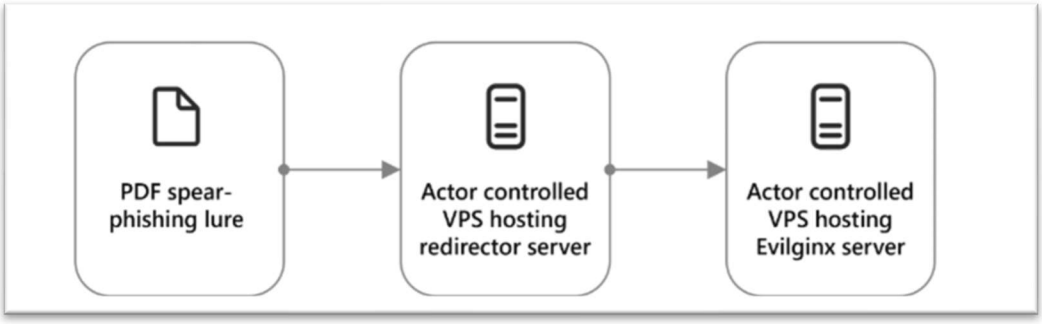


Figure 10

32. On occasion, Microsoft has observed attempts by the Star Blizzard Defendants to evade automated browsing and detonation by fingerprinting browsing behavior. In automated browsing, security systems use automated tools to visit websites. "Detonation" is when those security systems open files to see if they are harmful (like scanning them to see if they have a virus). Just like a fingerprint is unique, every browser and user have a unique "fingerprint" based on how users browse the Internet. The Star Blizzard Defendants can recognize when a security tool is checking their malicious website or file and limit malicious activity to avoid raising any alarms.

33. Once the target is redirected to the final page, the target is prompted to enter their credentials, by proxying the connect to the sign-in page for a legitimate provider and intercepting any credentials and authentication tokens. After credentials are captured or authentication tokens copied, the target is redirected to a website or document to complete the interaction to prevent tipping off the target that a phishing attack occurred. **Figure 11** is an example of a cloned phishing portal used by the Star Blizzard Defendants to directly impersonate a victim organization.

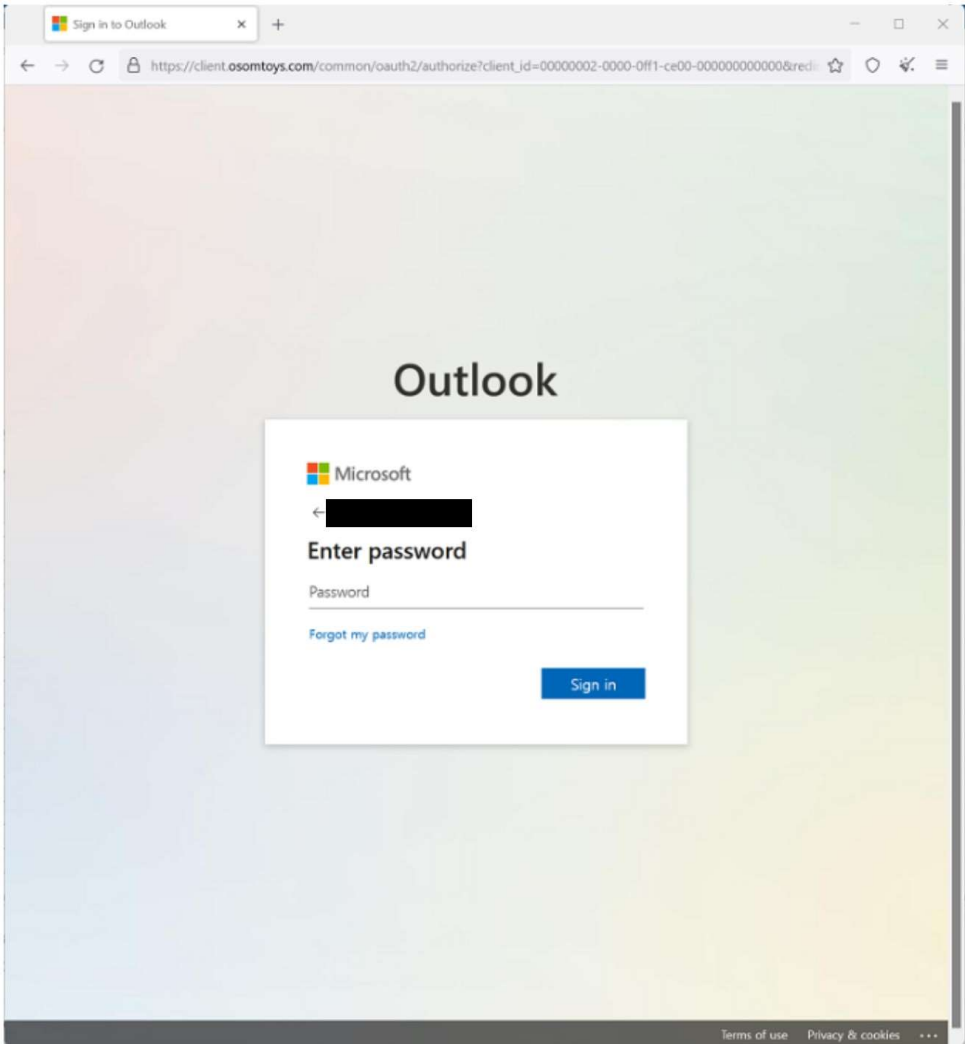


Figure 11

Attack Step 4: Use Credentials and Exfiltrated Data

34. Our investigation showed that the Star Blizzard Defendants use stolen credentials and replayed authentication tokens to directly sign in to victim email accounts. We have confirmed that Defendants regularly engage in the following activities:

a. **Exfiltration of intelligence data**: Defendants access exfiltrate emails, attachments, and contact lists from the inbox of victims. This includes both the ability to view

the sensitive data within the email inbox and to download contact lists, emails, and any attachments to those emails.

b. **Setup of persistent data collection**: In limited cases, the Star Blizzard Defendants set up forwarding rules from victim inboxes to Star Blizzard-controlled dead drop accounts where the actor has long-term access to collected data. On more than one occasion, we have observed that the Star Blizzard Defendants were able to access mailing list data for sensitive groups, such as those frequented by former intelligence officials, and maintain a collection of information from the mailing list for targeting and exfiltration.

c. **Access to people of interest**: There have been several cases where the Star Blizzard Defendants used their impersonation accounts to facilitate dialog with specific people of interest and, as a result, were included in conversations, sometimes unwittingly, involving multiple parties. The nature of the conversations identified during investigations by Microsoft demonstrates potentially sensitive information being shared that could provide intelligence value.

35. Based on the specific victimology, documents stolen, conversations fostered, and sustained collection observed, we assess that data theft is likely a key motivation of the Star Blizzard Defendants.

IV. INVESTIGATING THE STAR BLIZZARD INTERNET INFRASTRUCTURE

36. Microsoft investigated the online infrastructure used in the Star Blizzard Defendants' spear phishing campaign described in this declaration. We determined that Defendants have registered Internet domains using fictitious names and fictitious physical addresses that are purportedly located in multiple cities and countries. The Star Blizzard

Defendants have registered domains using functioning email addresses by which they communicated with domain registrars in order to complete the registration process.

37. Cybercriminals like the Star Blizzard Defendants are known to obfuscate their identities to evade capture by law enforcement and continue their cybercrime, which in this instance, is to engage in spear phishing activities to steal personal information and exfiltrate sensitive data.

38. In the course of the investigation, Microsoft (1) engaged in the analysis and creation of "signatures" (which can be thought of as digital fingerprints) for the infrastructure used by the Defendants, (2) discovered login activity into Microsoft services from Star Blizzard-controlled infrastructure on the Internet, (3) matched reported Star Blizzard spear phishing campaigns to registered domains, (4) monitored domain registrations associated with the Star Blizzard-controlled email addresses and other pertinent WHOIS record information, (5) monitored infrastructure frequently utilized by the Star Blizzard defendants in order to identify new domains being registered by the Star Blizzard defendants, (6) has confirmed resolution settings to particular proxy systems hosted on Virtual Private Servers (VPSs) which have frequently been used by the Star Blizzard defendants in the past, and (7) reviewed peer findings and public reporting.

39. For example, among other factors, Microsoft monitors and utilizes features specifically used by the Defendants, dates associated with the domain (registration etc.), particular abuse types or infrastructure providers previously seen carried out by the Star Blizzard Defendants, re-use of technical infrastructure previously used by the Defendants (specific Internet Protocol (IP) addresses and similar technical features associated with the domain or its operation), particular patterns of domain naming conventions that are known to be associated with the Defendants.

40. Our investigation found that the Star Blizzard Defendants register custom deceptive domains name that mimics a known website or cloud service may help the spear phishing link appear legitimate if securitized by the recipient. They use bespoke domains sparingly to reduce the likelihood an email security gateway or desktop security software will block the use of the link. By using a custom domain name, the Star Blizzard Defendants control when and how it delivered material and allows control of the Domain Name Service (DNS)[3] settings for redirection to Star Blizzard-controlled IP addresses and proxies and filters which computers are redirected through the proxy. The Star Blizzard Defendants use these domains/IP addresses as infrastructure to deliver a custom-built weaponized PDF or files to lure for the victim into opening and providing their credentials to copy authentication tokens.

41. These features, when identified in the aggregate, provide a high level of confidence that a given domain is a Star Blizzard domain. Each such domain is manually reviewed in detail by one or more subject matter experts as necessary to ascertain whether it is, in fact, a Star Blizzard domain. Based on this analysis, we have identified characteristics of the registration and maintenance of certain domains which, when coupled with the nature of the activities observed being carried out through the domains, are a reliable method to correlate such domains to actions undertaken by the Star Blizzard Defendants. At times, other researchers in the security community independently identify Star Blizzard domains and associated IP addresses, and these reports may be used to further validate Microsoft's analysis.

[3] The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like Microsoft.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources. https://www.cloudflare.com/learning/dns/what-is-dns/.

42. Our investigation and analysis note that the Star Blizzard Defendants have attempted to obfuscate their identities by using email marketing platforms to hide true email sender addresses and privacy-focused DNS providers to obscure IP addresses.

43. The Star Blizzard Defendants also use server-side scripts, which performs a filtering capability, in an attempt to ensure that the only successful connection made to the backend AiTM proxy is the intended target, and not cyber security researchers/analysts/network defenders, by running software code that automates processes on network servers that are operated by Defendants. The Star Blizzard Defendants also use virtual private servers (VPS) and cloud-based file-sharing platforms.

V. DEFENDANTS ATTACKED MICROSOFT CUSTOMERS IN THE DC METROPOLITAN AREA

44. Through its investigation, Microsoft has determined that, through the attacks described in this declaration, the Star Blizzard Defendants have affirmatively targeted Microsoft customers in the D.C. metropolitan area.

45. Microsoft recently investigated the recent IP addresses used by the accounts known to be targeted by Star Blizzard's spear phishing activities. Technology exists to determine the geographic location of IP addresses, alone or in association with domains. Using such technology, I determined the geographical location of these IP addresses collected during the sample period. I plotted such IP addresses on maps of the District of Columbia (DC) metropolitan area (including the Northern Virginia area and parts of Maryland), to represent the location of the relevant activity.

46. As can be seen below, in **Figure 12**, the Star Blizzard Defendants have directed their spear phishing activity toward defense and intelligence consulting companies, non-

governmental organizations (NGOs) and intergovernmental organizations (IGOs), think tanks, and higher education in the District of Columbia.

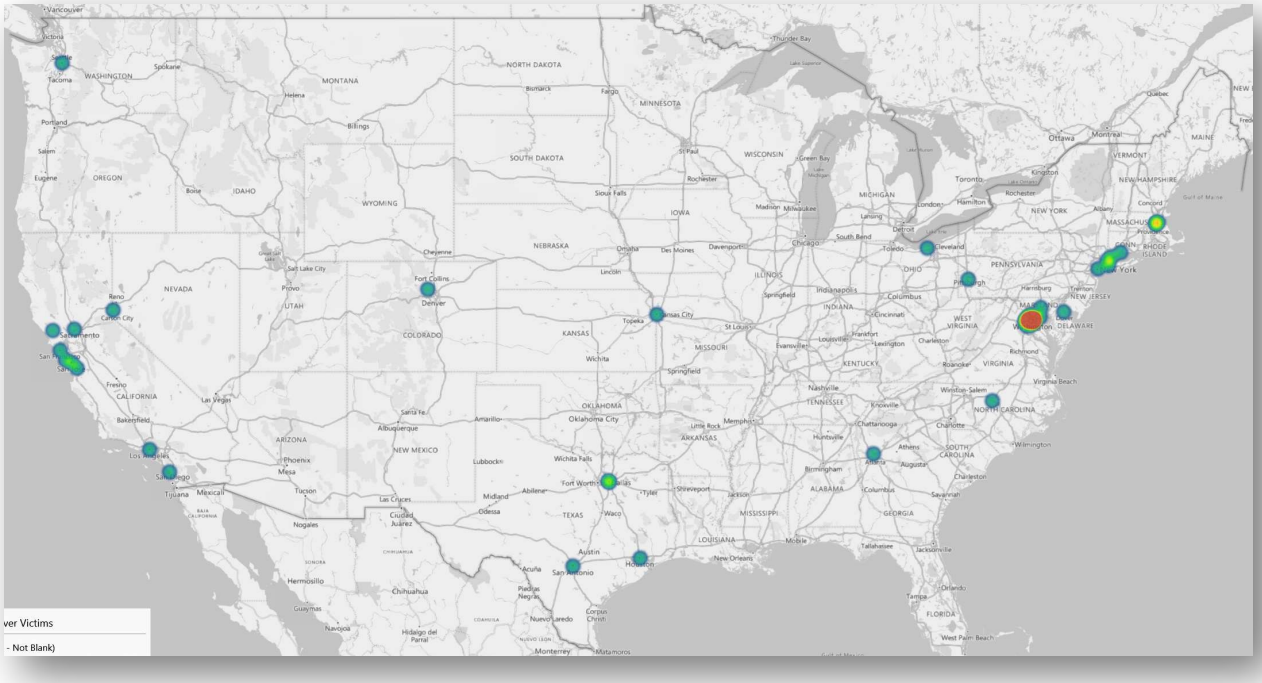


Figure 12

VI. HARM TO MICROSOFT AND ITS CUSTOMERS

47. The Star Blizzard Defendants' activities irreparably harm Microsoft by damaging its reputation, brands, and customer goodwill. Microsoft is the provider of the Windows operating system and Outlook, Hotmail, OneDrive and Office 365 email and cloud services, as well as a variety of other software and services. Microsoft is the owner of the "Microsoft," "Windows," "Office," and "Outlook" trademarks. Trademark registrations infringed by Defendants are attached to the Complaint as **Appendix B.** Microsoft has invested substantial resources in developing high-quality products and services. Due to the high quality and effectiveness of Microsoft's products

and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, has established a strong brand, and has developed the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. Microsoft has registered trademarks representing the quality of its products and service and its brand, including the trademarks listed above. Microsoft has invested significant resources in excess of $5,000 to address the harm caused by the Star Blizzard Defendants' activities. Specifically, Microsoft has expended approximately $1,000,000, which represents the Microsoft personnel involved in efforts to investigate the Star Blizzard Defendants and their infrastructure.

48. Microsoft's customers who receive malicious spear phishing emails in their Outlook, Hotmail or Office 365 email addresses are damaged by the Star Blizzard Defendants' activities. Customers whose email accounts are compromised through the Defendants' credential theft are damaged by these activities.

49. Customers are usually unaware of the fact that they are being targeted, that their email accounts are compromised, that they are being monitored by the Star Blizzard Defendants or that sensitive information is being stolen from them. Even if aware of an account intrusion, users often lack the technical resources or skills to resolve the problem, allowing their accounts to be misused indefinitely, as manual steps to change account credentials or remove the Star Blizzard Defendants' access may be difficult for ordinary users.

50. This demonstrates the extreme problems that the activities of the Star Blizzard Defendants cause for Microsoft's customers and the irreparable injury to both Microsoft and its customers. Microsoft and other members of the public must invest considerable time and resources investigating and remediating the defendants' intrusion into accounts and computers.

51. The activities of the Star Blizzard Defendants injure Microsoft and its reputation, brand, and goodwill. Defendants abuse Microsoft's terms of service and tarnish Microsoft's trademark. Customers subject to the negative effects of Defendants' spear phishing emails sometimes incorrectly believe that Microsoft is the source of the problem, and thus there is a significant risk that Microsoft customers will be confused in this way in the future. There is a great risk that Microsoft customers may incorrectly attribute these problems to Microsoft and associate these problems with Microsoft's products and services, thereby diluting and tarnishing the value of these trademarks and brands.

52. For customers in defense and intelligence consulting companies, non-governmental organizations (NGOs) and intergovernmental organizations (IGOs), think tanks, politicians, and higher education, the Star Blizzard Defendants' credential theft and exfiltration of data can be particularly damaging. Invasion of privacy, exfiltration of sensitive data, impersonation, reputational damage, ease of influence operations that may impact a targeted victim's career and how the public perceive their efforts, which may affect a victim's professional career.

53. Attached to this declaration as **Exhibit 3** is a true and correct copy of an article discussing Star Blizzard's activities expanding further to include defense-industrial targets, as well as U.S. Department of Energy facilities.[4]

VII. DISRUPTING STAR BLIZZARD'S ILLEGAL ACTIVITY

54. The most vulnerable point in the Defendants' operations are several Internet domains through which the Star Blizzard Defendants use AiTM proxies to obtain victim authentication tokens, replay those tokens to compromise accounts, and access sensitive

[4] Russian FSB accused of spear-phishing campaign against UK, US and allies, https://www.cshub.com/attacks/news/russian-fsb-accused-of-spear-phishing-campaign-against-uk-us-and-allies

information from victim accounts. A set of these is attached as **Appendix A** to the Complaint. These domains have been used in spear phishing emails directed at users of Microsoft's email services and exploit other Microsoft platforms like OneDrive.

55. Granting Microsoft possession of these domains will enable Microsoft to channel all communications to those domains to secure servers, and thereby cut off the means by which the Star Blizzard Defendants collect victim credentials. In other words, any time a user clicks on a link in a spear phishing email and provides their username and password, that information will be prevented from going to the Defendants at the Star Blizzard-controlled domains, because those domains will be hosted on a Microsoft-controlled, secure server, beyond the control of the Star Blizzard Defendants.

56. Redirecting these Star Blizzard domains will directly disrupt current infrastructure, mitigating risk and injury to Microsoft and its customers. The requested relief will also serve the public interest, in protecting customers of other web services companies who have consented to the relief sought in this action.

57. I believe that the most effective way to suspend the injury caused to Microsoft, its consumers, and the public, is to take the steps described in the Proposed Order. This relief will significantly hinder the Star Blizzard Defendants' ability to compromise additional accounts and identify new potential victims to target. In the absence of such action, the Defendants will be able to continue using this infrastructure to target new accounts, exposing potential new victims to Star Blizzard's malicious activities.

58. The Star Blizzard Defendants' techniques are designed to resist technical mitigation efforts, eliminating the ability to curb the injury purely through technical means. For example, once domains in the Star Blizzard Defendants' active infrastructure become known to the security

community, the Defendants abandon that infrastructure and move to new infrastructure that is used to continue Defendants' efforts to compromise accounts of new victims.

59. For this reason, providing notice to the Star Blizzard Defendants in advance of redirection of the domains at issue would render attempts to disable the infrastructure futile. Further, when the Defendants become aware of efforts to mitigate or investigate their activities, they take steps to conceal their activities and to conceal the injury that has been caused to victims, making it more difficult for victims to adequately assess the damage or take steps to mitigate that injury going forward. For this reason, as well, providing notice to the Star Blizzard Defendants in advance of redirection of the domains at issue would render attempts to mitigate the harm futile, or at least much more difficult for Microsoft.

60. Based on my experience observing the operation of numerous intrusions such as those carried out by the Star Blizzard Defendants, prior investigations, and legal actions involving such intrusions and actors, I believe that Defendants would take swift preemptive action to conceal the extent of the victimization of Microsoft and its customers and to defend their infrastructure, if they were to learn of Microsoft's impending action and request for relief.

61. I am informed and believe there have been prior instances where security researchers or the government attempted to curb injury caused by actors carrying out intrusions such as those in this case but allowed those actors to receive notice. In these cases, the actors quickly concealed the scope and nature of their intrusion, and moved the infrastructure to new, unidentified locations on the Internet and took other countermeasures causing the actors to continue their operations and destroying or concealing evidence of their operations.

62. For all of these reasons, I believe that the only way to mitigate injury and disrupt the most recent, active Star Blizzard infrastructure, is to redirect the domains at issue prior to providing notice to the Defendants.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct to the best of my knowledge.

Executed September 24, 2024, in Washington D.C.

Respectfully submitted,

_____

Sean Ensz

Principal Investigator, Digital Crimes Unit
Microsoft Corporation

SEAN ENSZ

EXPERTISE

Investigations / Forensics

Incident Response

E-Discovery

Network Security

Program Development

CERTIFICATIONS

CISSP – ISC2 #44830
GSEC - GIAC
EnCE – Guidance Software
ACE- Access Data
RHCE 4 - RedHat, Inc

EDUCATION

BACHELOR OF SCIENCE
Oklahoma State University
2001

CONTACT

405.234.7715

saensz@gmail.com

PROFILE

Senior cyber security professional with 25 years of investigations, computer forensics, and incident response experience.

EXPERIENCE

Senior Investigator

Microsoft Digital Crimes Uni | 2021 - Present

Primary Responsibilities Include

- Investigating high impact cloud-based cybercrime incidents for potential criminal referral
- Developing Business Email Compromise Threat Intelligence on transnational organized crime gangs
- Disruption of Nation State infrastructure

SSIRP Crisis Lead

Microsoft Security Response Center | 2018 - 2021

Primary Responsibilities Include

- Managing cross-company security incident response that have significant impact to customers, Microsoft operations, and brand
- Managing incidents that include 0-day product vulnerabilities, cloud service vulnerabilities, privacy breaches, and criminal or nation state intrusions
- Coordinating with company stakeholders that include CELA, DCU, Issues Management, and Customer Support

Digital Security Manager

Devon Energy Corporation | 2014 - 2018

Primary Responsibilities Include

- Leading a 15-member security team
- Leading the Devon Cyber Incident Response Team (DCIRT)
- Conducting Insider Threat investigations
- Overseeing $4.1 million annual operating budget
- Managing Security Operations of Next-Gen Firewalls, Email Security Gateways, Endpoint Security, and Authentication Services
- Managing Physical Security video and card access systems
- Managing vendor relationships

SEAN ENSZ

TRAINING

SANS

SEC401 - Security Essentials
SEC504 – Incident Handling
SEC564 – Red Team Operations
LEG523 – Law of Investigations
MGT535 – IR Team Management

FORENSICS

NW3C – Basic Data Recovery
NW3C – Advanced Data Recovery
EnCase – Incident Responses & Forensic Analysis
EnCase – EnCase Enterprise
ACCESS DATA – FTK Bootcamp

INCIDENT RESPONSE

CERT/SEI – Incident Handling Fundamentals
CERT/SEI – Advanced Incident Handling

IT

RedHat – RHCE Rapid Track Course
Cisco - Introduction to Networking Technologies and ICND

Director of Information Security

University of Oklahoma | 2013- 2014

Primary Responsibilities

- Representing Information Security functions to the Chief Information Office and various campus executive committees
- Leading 10-member security team; including 2 managers
- Managing budget and priorities for Incident Response, Computer Forensics, E-Discovery, and Risk Management functions
- Overseeing enterprise-wide information security programs
- Developing IT security related policy, process, and best practices
- Establishing and executing the university's strategic security initiatives

Accomplishments

- Established tri-campus security governance advisory council
- Advocated $2.4 million next-gen network security architecture
- Developed new campus-wide security risk management program

Principal Forensic Investigator

University of Oklahoma | 2004- 2013

Primary Responsibilities

- Conducting digital investigations for Human Resources, Sexual Misconduct Office, and Law Enforcement assistance
- Managing the OU Cyber Forensics Lab that maintained forensics capability for hard disk, mobile device, and network log analysis for IT and Police usage
- Coordinating E-discovery efforts: preserve, collect, and analyze electronic stored information in preparation for civil litigation
- Investigating network intrusions into campus system and data breaches and communicating findings to IT and campus leadership
- Designing and implementing network monitoring tools to assistant in Incident Response and digital investigations
- Team Lead for 6-person Investigations and Incident Response team

Accomplishments

- Established OU Cyber Forensics Lab used by IT Security, OU Police, and Norman Police
- Established the university's E-Discovery program in conjunction with the Office of Legal Counsel

SEAN ENSZ

TOOLS EXPERIENCE

Encase - Guidance Software

Forensics ToolKit - Access Data

Cellebrite UFED - Cellebrite

Office 365 Governance & Compliance - Microsoft

Maltego - Paterva

Qradar SIEM - IBM

Moloch Network Analysis - Open Source

Command Line Linux Tools - Open Souce

Police Investigator (*1999-2003)*

Police Officer (*1998-1999)*

Dispatcher (*1995-1998)*

Oklahoma State University Police Department | 1995- 2003

Primary Responsibilities

- Investigating computer crimes and other criminal violations as a State Commissioned Police Officer
- Conducting computer forensic investigations involving child pornography, network intrusions, credit card fraud, and intellectual property theft
- Investigating other criminal violations involving rape, narcotics, property theft, and fraud
- Providing investigative assistance to Federal Bureau of Investigations, Oklahoma State Bureau of Investigations, and Stillwater Police Dept

Accomplishments

- Established the OSUPD computer forensics lab
- Lead the investigation into the State's first successful prosecution of a digital copyright law violation

ADDITIONAL EXPERIENCE

Computer Forensics Adjunct Professor - Part Time

Redlands Community College / 2005 – 2007

Network Security Specialist

Oklahoma State University / 2003 – 2004

An official website of the United States government Here's how you know

CYBERSECURITY ADVISORY

Russian FSB Cyber Actor Star Blizzard Continues Worldwide Spear-phishing Campaigns

Release Date: December 07, 2023 **Alert Code:** AA23-341A

RELATED TOPICS: NATION-STATE CYBER ACTORS </topics/cyber-threats-and-advisories/nation-state-cyber-actors>, CYBER THREATS AND ADVISORIES </topics/cyber-threats-and-advisories>, MALWARE, PHISHING, AND RANSOMWARE </topics/cyber-threats-and-advisories/malware-phishing-and-ransomware>

The Russia-based actor is targeting organizations and individuals in the UK and other geographical areas of interest.

OVERVIEW

The Russia-based actor Star Blizzard (formerly known as SEABORGIUM, also known as Callisto Group/TA446/COLDRIVER/TAG-53/BlueCharlie) continues to successfully use spear-phishing attacks against targeted organizations and individuals in the UK, and other geographical areas of interest, for information-gathering activity.

The UK National Cyber Security Centre (NCSC), the US Cybersecurity and Infrastructure Security Agency (CISA), the US Federal Bureau of Investigation (FBI), the US National Security Agency (NSA), the US Cyber National Mission Force (CNMF), the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), the Canadian Centre for Cyber Security (CCCS), and the New Zealand National Cyber Security Centre (NCSC-NZ) assess that Star Blizzard is almost certainly subordinate to the Russian Federal Security Service (FSB) Centre 18.

Industry has previously published details of Star Blizzard. This advisory draws on that body of information <https://www.microsoft.com/en-us/security/blog/2022/08/15/disrupting-seaborgiums-ongoing-phishing-operations/>.

This advisory raises awareness of the spear-phishing techniques Star Blizzard uses to target individuals and organizations. This activity is continuing through 2023.

To download a PDF version of this advisory, see Russian FSB Cyber Actor Star Blizzard Continues Worldwide Spear-phishing Campaigns <https://www.ncsc.gov.uk/files/advisory-russian-fsb-cyber-actor-star-blizzard-continues-worldwide-spear-sphishing-campaigns.pdf>.

TARGETING PROFILE

Since 2019, Star Blizzard has targeted sectors including academia, defense, governmental organizations, NGOs, think tanks and politicians.

Targets in the UK and US appear to have been most affected by Star Blizzard activity, however activity has also been observed against targets in other NATO countries, and countries neighboring Russia.

During 2022, Star Blizzard activity appeared to expand further, to include defense-industrial targets, as well as US Department of Energy facilities.

OUTLINE OF THE ATTACKS

The activity is typical of spear-phishing campaigns, where an actor targets a specific individual or group using information known to be of interest to the targets. In a spear-phishing campaign, an actor perceives their target to have direct access to information of interest, be an access vector to another target, or both.

Research and Preparation

Using open-source resources to conduct reconnaissance, including social media and professional networking platforms, Star Blizzard identifies hooks to engage their target. They take the time to research their interests and identify their real-world social or professional contacts [T1589 <https://attack.mitre.org/versions/v14/techniques/t1589/>], [T1593 <https://attack.mitre.org/versions/v14/techniques/t1593/>].

Star Blizzard creates email accounts impersonating known contacts of their targets to help appear legitimate. They also create fake social media or networking profiles that impersonate respected experts [T1585.001 <https://attack.mitre.org/versions/v14/techniques/t1585/001/>] and have used supposed conference or event invitations as lures.

Star Blizzard uses webmail addresses from different providers, including Outlook, Gmail, Yahoo and Proton mail in their initial approach [T1585.002 <https://attack.mitre.org/versions/v14/techniques/t1585/002/>], impersonating known contacts of the target or well-known names in the target's field of interest or sector.

To appear authentic, the actor also creates malicious domains resembling legitimate organizations [T1583.001 <https://attack.mitre.org/versions/v14/techniques/t1583/001/>].

Microsoft Threat Intelligence Center (MSTIC) provides a list of observed Indicators of Compromise (IOCs) in their SEABORGIUM blog, but this is not exhaustive.

Preference for Personal Email Addresses

Star Blizzard has predominantly sent spear-phishing emails to targets' personal email addresses, although they have also used targets' corporate or business email addresses. The actors may intentionally use personal emails to circumvent security controls in place on corporate networks.

Building a Rapport

Having taken the time to research their targets' interests and contacts to create a believable approach, Star Blizzard now starts to build trust. They often begin by establishing benign contact on a topic they hope will engage their targets. There is often some correspondence between attacker and target, sometimes over an extended period, as the attacker builds rapport.

Delivery of Malicious Link

Once trust is established, the attacker uses typical phishing tradecraft and shares a link [T1566.002 <https://attack.mitre.org/versions/v14/techniques/t1566/002/>], apparently to a document or website of interest. This leads the target to an actor-controlled server, prompting the target to enter account credentials.

The malicious link may be a URL in an email message, or the actor may embed a link in a document [T1566.001 <https://attack.mitre.org/versions/v14/techniques/t1566/001/>] on OneDrive, Google Drive, or other file-sharing platforms <https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag/>.

Star Blizzard uses the open-source framework EvilGinx in their spear- phishing activity, which allows them to harvest credentials and session cookies to successfully bypass the use of two-factor authentication [T1539 <https://attack.mitre.org/versions/v14/techniques/t1539/>], [T1550.004 <https://attack.mitre.org/versions/v14/techniques/t1550/004/>].

Exploitation and Further Activity

Whichever delivery method is used, once the target clicks on the malicious URL, they are directed to an actor-controlled server that mirrors the sign-in page for a legitimate service. Any credentials entered at this point are now compromised.

Star Blizzard then uses the stolen credentials to log in to a target's email account [T1078 <https://attack.mitre.org/versions/v14/techniques/t1078/>], where they are known to access and steal emails and attachments from the victim's inbox [T1114.002 <https://attack.mitre.org/versions/v14/techniques/t1114/002/>]. They have also set up mail-forwarding rules, giving them ongoing visibility of victim correspondence [T1114.003 <https://attack.mitre.org/versions/v14/techniques/t1114/003/>].

The actor has also used their access to a victim email account to access mailing-list data and a victim's contacts list, which they then use for follow- on targeting. They have also used compromised email accounts for further phishing activity [T1586.002 <https://attack.mitre.org/versions/v14/techniques/t1586/002/>].

CONCLUSION

Spear-phishing is an established technique used by many actors, and Star Blizzard uses it successfully, evolving the technique to maintain their success.

Individuals and organizations from previously targeted sectors should be vigilant of the techniques described in this advisory.

In the UK you can report related suspicious activity to the NCSC <https://report.ncsc.gov.uk/>.

Information on effective defense against spear-phishing is included in the Mitigations section below.

MITRE ATT&CK®

This report has been compiled with respect to the MITRE ATT&CK® <https://attack.mitre.org/versions/v14/matrices/enterprise/> framework, a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

Tactic	ID	Technique	Procedure
Reconnaissance	T1593 <https://attack.mitre.org/versions/v14/techniques/t1593/>	Search Open Websites/Domains	Star Blizzard uses open-source resear and social media to identify information about victims use in targeting.
Reconnaissance	T1589 <https://attack.mitre.org/versions/v14/techniques/t1589/>	Gather Victim Identity Information	Star Blizzard uses online data sets and open-source resources to gather information about their targets.
Resource Development	T1585.001 <https://attack.mitre.org/versions/v14/techniques/t1585/001/>	Establish Accounts: Social Media Accounts	Star Blizzard has been observed establishing fraudulent profiles on professional networking sites to condu reconnaissan
Resource Development	T1585.002 <https://attack.mitre.org/versions/v14/techniques/t1585/002/>	Establish Accounts: Email Accounts	Star Blizzard registers consumer em accounts matching the names of individuals th are impersonatin to conduct spear-phishin activity.

Tactic	ID	Technique	Procedure
Resource Development	T1583.001 <https://attack.mitre.org/versions/v14/techniques/t1583/001/>	Acquire Infrastructure: Domains	Star Blizzard registers domains to hc their phishing framework.
Resource Development	T1586.002 <https://attack.mitre.org/versions/v14/techniques/t1586/002/>	Compromise Accounts: Email Accounts	Star Blizzard has been observed usir compromised victim email accounts to conduct spea phishing activity again contacts of th original victir
Initial Access	T1078 <https://attack.mitre.org/versions/v14/techniques/t1078/>	Valid Accounts	Star Blizzard uses compromised credentials, captured from fake log-in pages, to log i to valid victim user accounts
Initial Access	T1566.001 <https://attack.mitre.org/versions/v14/techniques/t1566/001/>	Phishing: Spear-phishing Attachment	Star Blizzard uses maliciou links embedd in email attachments t direct victims their credenti stealing sites
Initial Access	T1566.002 <https://attack.mitre.org/versions/v14/techniques/t1566/002/>	Phishing: Spear-phishing Link	Star Blizzard sends spear-phishing ema with maliciou links directly credential-stealing sites or to documer hosted on a fi sharing site, which then direct victims credential-stealing sites

Tactic	ID	Technique	Procedure
Defense Evasion	T1550.004 <https://attack.mitre.org/versions/v14/techniques/t1550/004/>	Use Alternate Authentication Material: Web Session Cookie	Star Blizzard bypasses mul factor authenticatio on victim ema accounts by using session cookies stole using EvilGin
Credential Access	T1539 <https://attack.mitre.org/versions/v14/techniques/t1539/>	Steal Web Session Cookie	Star Blizzard uses EvilGinx steal the session cooki of victims directed to th fake log-in domains.
Collection	T1114.002 <https://attack.mitre.org/versions/v14/techniques/t1114/002/>	Email Collection: Remote Email Collection	Star Blizzard interacts directly with externally facing Exchange services, Offi 365 and Goog Workspace to access email and steal information using compromised credentials or access token
Collection	T1114.003 <https://attack.mitre.org/versions/v14/techniques/t1114/003/>	Email Collection: Email Forwarding Rule	Star Blizzard abuses email- forwarding rules to monit the activities a victim, steal information, and maintain persistent access to victim's email even after compromised credentials ar reset.

MITIGATIONS

A number of mitigations will be useful in defending against the activity described in this advisory.

- **Use strong passwords. Use a separate password for email accounts and avoid password re-use across multiple services.** See NCSC guidance: Top Tips for Staying Secure Online <https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/use-a-strong-and-separate-password-for-email>.
- **Use multi-factor authentication** (2-factor authentication/two-step authentication) to reduce the impact of password compromises. See NCSC guidance: Multi-factor Authentication for Online Services <https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services> and Setting Up 2-Step Verification (2SV) <https://www.ncsc.gov.uk/guidance/setting-2-step-verification-2sv>.
- **Protect your devices and networks by keeping them up to date:** Use the latest supported versions, apply security updates promptly, use anti-virus and scan regularly to guard against known malware threats. See NCSC guidance: Device Security Guidance <https://www.ncsc.gov.uk/collection/device-security-guidance/policies-and-settings/antivirus-and-other-security-software>.
- **Exercise vigilance.** Spear-phishing emails are tailored to avoid suspicion. You may recognize the sender's name, but has the email come from an address that you recognize? Would you expect contact from this person's webmail address rather than their corporate email address? Has the suspicious email come to your personal/webmail address rather than your corporate one? Can you verify that the email is legitimate via another means? See NCSC guidance: Phishing attacks: Defending Your Organization <https://www.ncsc.gov.uk/guidance/phishing> and Internet Crime Complaint Center(IC3) | Industry Alerts <https://www.ic3.gov/home/industryalerts>.
- **Enable your email providers' automated email scanning features.** These are turned on by default for consumer mail providers. See NCSC guidance: Telling Users to "Avoid Clicking Bad Links" Still Isn't Working <https://www.ncsc.gov.uk/blog-post/telling-users-to-avoid-clicking-bad-links-still-isnt-working>.
- **Disable mail-forwarding.** Attackers have been observed to set up mail-forwarding rules to maintain visibility of target emails. If you cannot disable mail-forwarding, then monitor settings regularly to ensure that a forwarding rule has not been set up by an external malicious actor.

DISCLAIMER

This report draws on information derived from NCSC and industry sources. Any NCSC findings and recommendations made have not been provided with the intention of avoiding all risks and following the recommendations will not remove all such risk. Ownership of information risks remains with the relevant system owner at all times.

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation.

Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.

All material is UK Crown Copyright©.

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

Tags

Topics: Nation-State Cyber Actors </topics/cyber-threats-and-advisories/nation-state-cyber-actors>, Cyber Threats and Advisories </topics/cyber-threats-and-advisories>, Malware, Phishing, and Ransomware </topics/cyber-threats-and-advisories/malware-phishing-and-ransomware>

MITRE ATT&CK TTP: Collection (TA0009), Credential Access (TA0006), Defense Evasion (TA0005), Initial Access (TA0001), Reconnaissance (TA0043), Resource Development (TA0042)

Co-Sealers and Partners: Federal Bureau of Investigation, International, National Security Agency

Nation-State Actor: Russia

Please share your thoughts

We recently updated our anonymous product survey; we'd welcome your feedback.

Related Advisories

SEP 05, 2024 **CYBERSECURITY ADVISORY | AA24-249A**

Russian Military Cyber Actors Target US and Global Critical Infrastructure </news-events/cybersecurity-advisories/aa24-249a>

AUG 29, 2024 **CYBERSECURITY ADVISORY | AA24-242A**

#StopRansomware: RansomHub Ransomware </news-events/cybersecurity-advisories/aa24-242a>

AUG 28, 2024 **CYBERSECURITY ADVISORY | AA24-241A**

Iran-based Cyber Actors Enabling Ransomware Attacks on US Organizations </news-events/cybersecurity-advisories/aa24-241a>

JUL 25, 2024 **CYBERSECURITY ADVISORY | AA24-207A**

North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs </news-events/cybersecurity-advisories/aa24-207a>

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools> **News & Events** </news-events>

Careers </careers> **About** </about>

CISA Central

1-844-Say-CISA SayCISA@cisa.dhs.gov

CISA.gov
An official website of the U.S. Department of Homeland Security

About CISA </about>

Budget and Performance <https://www.dhs.gov/performance-financial-reports>

DHS.gov <https://www.dhs.gov>

Equal Opportunity & Accessibility </oedia>

FOIA Requests <https://www.dhs.gov/foia>

No FEAR Act </no-fear-act>

Office of Inspector General <https://www.oig.dhs.gov/>

Privacy Policy </privacy-policy>

Subscribe

The White House <https://www.whitehouse.gov/>

USA.gov <https://www.usa.gov/>

Website Feedback </forms/feedback>

Filter Categories +

Russian FSB accused of spear-phishing campaign against UK, US and allies

Star Blizzard threat actor is “almost certainly” subordinate to the Russian Federal Security Service Centre 18

Add bookmark

Michael Hill

12/08/2023

The Russia-based actor Star Blizzard (formerly known as SEABORGIUM) continues to successfully use spear-phishing attacks against targeted organizations and individuals in the UK and US, as well as other geographical areas of interest, for information-gathering activity. That’s according to an international cyber security advisory from multiple governments which states that Star Blizzard (also known as Callisto Group/TA446/COLDRIVER/TAG-53/BlueCharlie) is almost certainly subordinate to the Russian Federal Security Service (FSB) Centre 18.

Star Blizzard has targeted sectors including academia, governmental organizations, NGOs, think tanks and politicians since 2019. Targets in the UK and US appear to have been most affected by Star Blizzard activity, however activity has also been observed against targets in other NATO countries and neighboring Russia, the advisory read. More recently, Star Blizzard activity appeared to expand further to include defense-industrial targets, as well as US Department of Energy facilities.

The UK Foreign Office has summoned the Russian ambassador and sanctioned a Russian intelligence officer along with a second member of the Star Blizzard group, according to *Sky News*. The UK government said the malicious cyber activity is an attempt to interfere in UK politics and democratic processes.

Star Blizzard conducts reconnaissance and impersonates contacts of their targets

Using open-source resources to conduct reconnaissance, including social media and professional networking platforms, Star Blizzard identifies hooks to engage targets, the advisory stated. “They take the time to research their interests and identify their real-world social or professional contacts.”

The threat actor creates email accounts impersonating known contacts of their targets to help appear legitimate. “They also create fake social media or networking profiles that impersonate respected experts and have used supposed conference or event invitations as lures.” Star Blizzard uses webmail addresses from different providers including Outlook, Gmail, Yahoo and Proton mail in their initial approach.

Personal email addresses targeted with spear-phishing

Star Blizzard has predominantly sent spear-phishing emails to targets’ personal email addresses, although they have also used targets’ corporate or business email addresses, the government said. “The actors may intentionally use personal emails to circumvent security controls in place on corporate networks.”

Having researched their targets’ interests and contacts to create a believable approach, Star Blizzard then starts to build trust with potential victims. “They often begin by establishing benign contact on a topic they hope will engage their targets. There is often some correspondence between attacker and target, sometimes over an extended period, as the attacker builds rapport.”

Once trust is established, the attacker uses typical phishing tradecraft and shares a link, apparently to a document or website of interest. This leads the target to an actor-controlled server, prompting the target to enter account credentials. “The malicious link may be a URL in an email message, or the actor may embed a link in a document on OneDrive, Google Drive or other file-sharing platforms.”

Threat actor uses open-source framework to harvest credentials and session cookies

Star Blizzard uses the open-source framework EvilGinx to harvest credentials and session cookies, successfully bypassing the use of two-factor authentication (2FA). Once the target clicks on the malicious URL, they are directed to an actor-controlled server that mirrors the sign-in page for a legitimate service. Any credentials entered at this point are now compromised.

“Star Blizzard then uses the stolen credentials to log in to a target’s email account, where they are known to access and steal emails and attachments from the victim’s inbox. They have also set up mail-forwarding rules, giving them ongoing visibility of victim correspondence.”

Furthermore, the actor has used their access to a victim email account to access mailing-list data and a victim’s contacts list, which they then use for follow-on targeting. They have also used compromised email accounts for further phishing activity.

A number of mitigations will be useful in defending against the activity, the advisory stated. These include:

- Using multi-factor authentication (MFA) to reduce the impact of password compromises.
- Protecting devices and networks by keeping them up to date.
- Enabling email providers’ automated email scanning features.
- Disabling mail-forwarding.

Revelations of Russian state-sponsored activity are no surprise

The revelations detailing alleged Russian state-sponsored attempts to influence democratic processes should come as no surprise, commented Chris Morgan, senior cyber threat intelligence analyst at cyber security firm ReliaQuest. “For several years, multiple Western countries have accused Russia of attempting to conduct espionage against its adversaries, sowing disinformation and otherwise seeking to undermine democratic processes. Such covert activities also allow Russia to extract sensitive information, maintain persistence within systems of organizations of strategic interest and obtain intelligence to guide Russian foreign policy.”

The attribution to StarBlizzard is also not unexpected, Morgan said. “The group has previously used domain impersonation to facilitate theft of credentials, while regularly rotating their infrastructure to avoid detection. Despite being agile and sophisticated, such APT groups continue to use rudimentary techniques – largely because they work.”

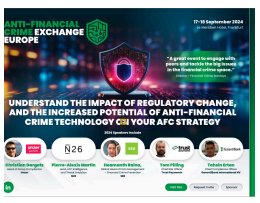
Tags: Cyber Attack Phishing Cyber Security Incident

Comments

You must Login or Subscribe to comment.

Upcoming Events

Anti-Financial Crime Exchange Europe 2024
September 19-20
Frankfurt, Germany
Register Now | View Agenda | View Event



OT Cybersecurity Summit
October 28 - 29, 2024
Norris Conference Center, Houston CityCentre, TX
Register Now | View Agenda | View Event

Automotive Cyber Security Europe 2024 | Automotive IQ
11 - 14 November 2024
The Westin Grand Frankfurt, Germany
Register Now | View Agenda | View Event

Digital Identity Week
09 - 10 September, 2025
Sydney, Australia
Register Now | View Agenda | View Event

MORE EVENTS

Follow Us

Subscribe to our Free Newsletter

Insights from the world's foremost thought leaders delivered to your inbox.

SUBSCRIBE

Latest Webinars

[Preventing financial and reputational risk with process intelligence](#)

2024-05-23

11:00 AM - 12:00 PM EDT

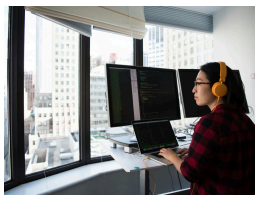
Learn how to manage risk stemming from poorly controlled processes in a collaborative way

[Building high-performing development teams: Harnessing tools, processes & AI](#)

2024-05-02

11:00 AM - 12:00 PM EDT

Discover how to enhance your development team's efficiency through advanced tools, Agile methodologi...



[Building cyber resilience](#)

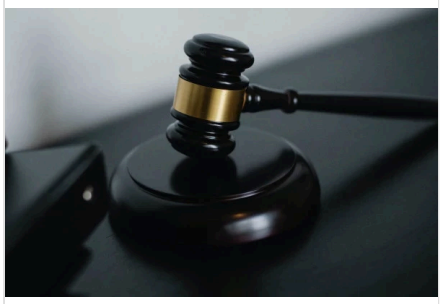
2024-04-24

11:30 AM - 12:30 PM SGT

Why it's essential that technology seamlessly connects IT, security, risk and the business

MORE WEBINARS

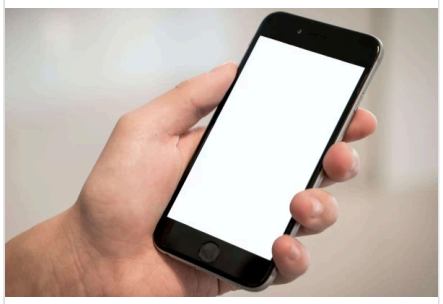
RECOMMENDED



[IOTW: Victoria Court recordings exposed in suspected ransomware attack](#)

2024-01-05

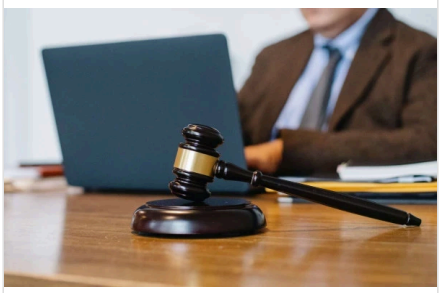
By [Michael Hill](#)



[IOTW: Russia-linked cyber attack targets Ukraine's biggest phone operator](#)

2023-12-15

By [Michael Hill](#)



[BEC attacks on law firms spike as cyber criminals bypass MFA](#)

2023-12-07

By [Michael Hill](#)

[IOTW: Data breach exposes sensitive information of Canadian Government employees](#)

2023-11-24

By [Michael Hill](#)

FIND CONTENT BY TYPE

News
Interviews
Videos
Case Studies
White Papers

CYBER SECURITY HUB COMMUNITY

About Us
Contact Us
Cookie Policy
Become a Contributor
Become a Member Today
Power10
Advertise with us
User Agreement
All Access from CS Hub
Media Partners

ADVERTISE WITH US

Reach Cyber Security professionals through cost-effective marketing opportunities to deliver your message, position yourself as a thought leader, and introduce new products, techniques and strategies to the market.

Advertise Now

JOIN THE CYBER SECURITY HUB COMMUNITY

Join CSHUB today and interact with a vibrant network of professionals, keeping up to date with the industry by accessing our wealth of articles, videos, live conferences and more.

Learn more

Cyber Security Hub, a division of IQPC

© 2024 All rights reserved. Use of this site constitutes acceptance of our User Agreement, Privacy Policy and Cookies Settings.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Microsoft Corporation, a Washington State Corporation, NGO-ISAC, a New York State Non-Profit Organization, Plaintiffs, v. John Does 1-2, Controlling A Computer Network and Thereby Injuring Plaintiff and Its Customers, Defendants.	Civil Action No. **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5.1**

DECLARATION OF IAN GOTTESMAN IN SUPPORT OF APPLICATION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, Ian Gottesman, declare as follows:

1. I am the Chief Executive Officer of the NGO Information Sharing and Analysis Center ("NGO-ISAC"), which is a Plaintiff in this action. I make this declaration in support of Plaintiffs' Application for an Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause re Preliminary Injunction. I make this declaration of my own personal knowledge or on information and belief where noted. If called as a witness, I could and would testify to the truth of the matters set forth herein.

2. I joined NGO-ISAC as CEO in April 2024. In my role at NGO-ISAC, I am responsible for leading and managing the organization's operations, strategic planning, and development initiatives. This includes ensuring that NGO-ISAC effectively serves its members in the nonprofit sector by providing critical information sharing and analysis services related to cybersecurity threats, vulnerabilities, capacity building, policy implementation. I lead our organization in ensuring the delivery of timely and relevant cybersecurity information and analysis

to our members and oversee the development and implementation of tools and resources to support member organizations in managing cybersecurity and adjacent risks. My role also includes policy and advocacy work such as engaging in policy development and advocacy efforts related to cybersecurity in the nonprofit sector. Additionally, I collaborate with policymakers, industry leaders, and other ISACs to promote best practices and standards.

3. Prior to joining NGO-ISAC, I served as the Chief Information Officer for the Carnegie Endowment for International Peace ("CEIP"), which is a global nonprofit with four international centers providing strategic insight that advance international peace where I worked to reduce ongoing cybersecurity threats to the organization's communication and research efforts. I also served as the Chief Information Officer for Center for Strategic and International Studies ("CSIS"), which is a bipartisan think tank that develops foreign and defense policy solutions for the federal government. A current version of my curriculum vitae is attached to this declaration as **Exhibit 1.**

I. NGO-ISAC

4. NGO-ISAC is a 501(c)(3) nonprofit corporation duly organized and existing under the laws the state of New York and having its headquarters and principal place of business in Alexandria, Virginia. NGO-ISAC elevates the cybersecurity posture of US-based nonprofits and non-governmental organizations ("NGO")[1] through information sharing, training and education programs, and specialized cybersecurity consulting services, all tailored to empower and protect

[1] For the purposes of this declaration, the term "NGO" will encompass both NGOs and nonprofits. An **NGO** is an organization that is not part of the government, but help provide humanitarian aid and advocate for social change. They may also operate in the same areas that government agencies do, but they are not part of the government. NGOs can exist at the local, national, or international level. In most cases, they either operate internationally or are based in the US, but provide services across borders. A **nonprofit** organization has missions to help a specific cause or community. Nonprofits may operate on a small-scale, like within a community, or on a broader scale, like nationwide. When comparing an NGO to a nonprofit, it is useful to know that most NGOs are also nonprofits. However, only some nonprofits are NGOs. A nonprofit can be an NGO when it operates on a larger scale.

nonprofits. NGO-ISAC is a membership organization comprised of representatives from NGOs that collaborate to improve the security of U.S.-based organizations. The organization and its members drive robust, effective cybersecurity programs in NGOs through capacity and community-building by sharing intelligence, promoting best practices, and facilitating educational events. NGO-ISAC offers a range of cybersecurity consulting services to help members assess and improve their digital security, including conducting vulnerability assessments to policy development to help keep organizations stay safe and secure. NGO-ISAC serves organizations directly, supporting in a virtual Chief Information Security Officer (CISO) capacity and mentorship for members to help harden cyber and digital posture of NGOs and to make sure incident preparedness is in place. When an incident occurs, NGO-ISAC coaches the organization through the incident. We also offer training and education services to help organizations develop a culture of strong cybersecurity practices. NGO-ISAC also (i) facilitates connections between organizations with vendor contacts, (ii) facilitates information sharing among organization members, and (iii) provide a platform for collaboration and knowledge exchange.

5. NGO-ISAC has worked with over 200 NGOs in the United States to improve their cybersecurity. These member organizations work in important areas such as human rights, peace and disarmament, and scientific research on diseases. This work often requires a private or secure environment and any threat to that security impacts their ability to achieve their mission. In collaboration with our members, we have helped discover things that have impacted our whole sector large companies, and billions of users such as zero-days, and other cybersecurity issues that have affected our members, and users of those tools throughout the world.

II. OVERVIEW OF THE STAR BLIZZARD THREAT

6. My declaration concerns the spear-phishing attacks targeting nonprofits and NGOs, and as it applies here, regarding the Star Blizzard phishing operation. *See* Declaration of Sean Ensz in Support of Plaintiffs' Application For An Emergency Ex Parte Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("Ensz Decl.") ¶ 1. Star Blizzard Defendants are believed to run a Russia-based operation that engages in spear phishing resulting in the online impersonation of individuals and organizations, the infiltration of email accounts, and the exfiltration of sensitive and confidential information from those online accounts. Complaint ¶ 3. Star Blizzard Defendants are formerly known as SEABORGIUM and also known in the cybersecurity community as the Callisto Group, COLDRIVER, and BlueCharlie.

7. According to Microsoft's investigations, the Star Blizzard Defendants' campaigns target over 30 organizations, in addition to personal accounts of people of interest. Star Blizzard Defendants primarily target NATO countries, particularly the United States and the United Kingdom, and other countries in the Baltics, the Nordics, and Eastern Europe. Complaint ¶ 18.

8. Microsoft has observed the Star Blizzard Defendants' campaigns continue to target NGOs, think tanks, government employees, and personal accounts belonging to current and former military and intelligence officials and policy advisors. The individuals targeted by these attacks predominately reside in the U.S., in and around the Washington, D.C. area. Complaint ¶ 14.

III. IMPACT ON NGOs

9. The phishing attacks orchestrated by Star Blizzard Defendants and threat actors like Star Blizzard Defendants have had a profound impact on the NGO and nonprofit community. These attacks have forced NGOs to divert resources from their core missions to address security efforts. The damage to trust and reputation can also have long-lasting effects on an organization's

ability to secure funding and maintain partnerships.

10. This diversion of resources for our members has had high costs well more than $5,000 for most of our member organizations. This has included NGOs hiring full time cybersecurity staff, purchasing expensive tools to protect their data, communication or online image, and training for every member of an organization. These costs can be hundreds of thousands or millions of dollars moving funds and staff time away from their mission driven work of curing diseases, bringing peace to war zones, or providing guidance to public policy decision makers. The costs skyrocket in the case of a breach or serious incident. This can require organizations to remove their connection to the internet for a period of days or weeks while they rebuild their infrastructure such as email or file sharing systems. This can require organizations to close during this period while breaches are remediated. Our members are resource scarce organizations dedicated to complicated and important causes that can be derailed by a cybersecurity incident. Cybersecurity issues harms their ability to do work costing them precious time, scarce funds, ruining reputations, or worse.

11. NGO-ISAC has led efforts to respond to phishing threats by providing our members with timely intelligence, best practice guidance, and coordination for incident response. NGO-ISAC works with cybersecurity agencies, other ISACs, and private sector partners to strengthen the collective defense against these advanced persistent threats.

12. On May 1, 2024, NGO-ISAC, in collaboration with the Cyber Threat Alliance, published the *2024 Cyber Threat to NGOs* Joint Analytic Report (JAR),[2] which serves as a call to action, comprehensive resource, and testament to industry leader collaboration. Amid the unique challenges facing NGOs – which, due to their involvement in sensitive political, governmental,

[2] Cyber Threat Alliance Publishes 2024 Cyber Threats To Ngos Joint Analytic Report, https://www.cyberthreatalliance.org/cyber-threats-to-ngos/.

and humanitarian areas, are exposed to a wider and more complex range of cyber threats than many commercial and governmental entities – the report outlines prevalent threats, suggests remediation strategies, and provides guidance on enhancing nonprofit cybersecurity posture. A true and correct copy of the report is attached to this declaration as **Exhibit 2.**

13. With limited resources, often large, distributed networks serving vulnerable populations, and involvement in sensitive political, governmental, and humanitarian areas, NGOs are attractive targets to cybercriminals. The top cyber threats to NGOs include financial theft, espionage, disinformation, and operational disruptions, with threat actors taking advantage of technical and social vulnerabilities such as fake websites, business email compromise, commercial and mercenary spyware, misinformation campaigns, social engineering, ransomware, and denial of service.

14. By virtue of being connected to the internet, NGOs are vulnerable to one of the most common kinds of cyber threats which involve variations of social engineering, including phishing, spear phishing, vishing, smishing, and business email compromise. The ongoing nature of these attacks necessitates immediate legal intervention to prevent further harm to NGOs. Protecting these organizations is essential to preserving their ability to carry out critical missions without the constant threat of cyber intrusions.

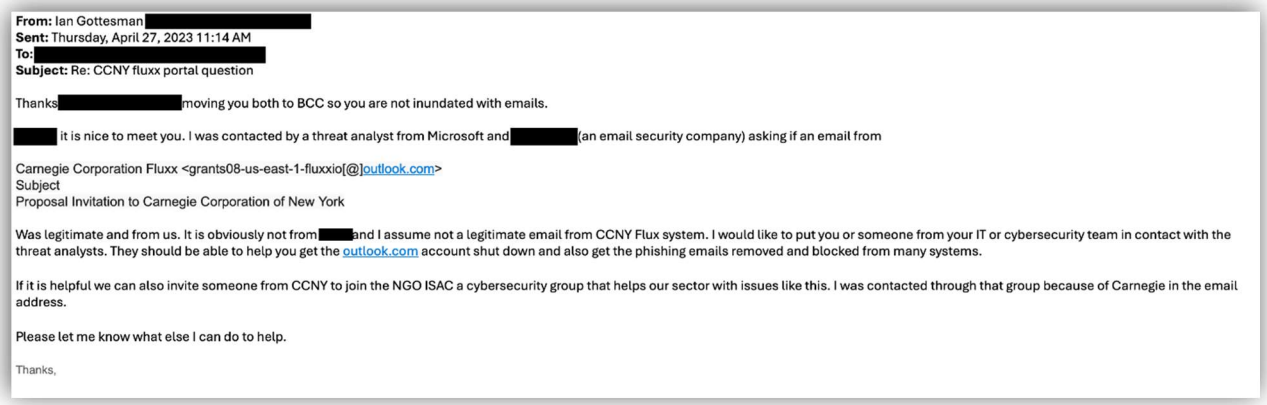
15. Social engineering threats exploit human psychology rather than technological vulnerabilities to gain unauthorized access to information or systems. Among the most common forms are phishing, spear phishing, smishing, and vishing. Phishing involves sending emails with malicious links or attachments under the guise of legitimate sources, targeting a broad audience without much personalization. Spear phishing, a more targeted version of phishing, focuses on individual recipients or specific entities within an organization, deploying well-researched and

highly credible threats that often lead to the deployment of malware.

16. Several NGO-ISAC members and partners have been targeted by Star Blizzard Defendants, including, for example, the Carnegie Corporation of New York ("the Corporation"), a proactive grantmaker that issues funding to invest in innovative projects that can have measurable impact on society and can create meaningful, transformative change related to issues on international peace, the advancement of education and knowledge, and democracy. *See* Declaration of Yotaro Sherman ("Yotaro Decl.") ¶ 4. The Star Blizzard Defendants have falsely used the Corporation's name, logo, mission, and confidential communications to target individual recipients or specific entities. This includes using specific, distinct information like grant numbers issued to grant recipients who received funding for projects.

17. On April 27, 2023, a threat analyst from Proofpoint contacted me in connection with an email that was purportedly sent by the Corporation's Fluxx, a grant management system (GMS) used by the Corporation and many other grant making organizations. At that time, I was employed by the Carnegie Endowment for International Peace ("CEIP"). As both organizations had Carnegie in the title, the email seemed odd, and I was active in the NGO-ISAC, I was contacted to see if I could provide any additional context to the message. The analyst also reached out concurrently to peers at Microsoft since the message was sent from an outlook.com email address. The sender's email address implied that it came from an official email address associated with the Fluxx grant management system. However, the sender's email address used an "outlook.com" domain, which is not consistent with a communication through the Fluxx grant management system. This indicates that this was not an authentic communication from the Fluxx grant management system. Through shared contacts at the NGO-ISAC I was able to find contact information for Yotaro Sherman. I shared the information I had gleaned from the email with Yotaro

and the corporation as well as other NGO-ISAC members as many of them were Corporation grantees that could be phished with similar emails or used Fluxx. Fluxx is the most common grant management system with many NGO ISAC members using it to both make and receive grants. Successful impersonation of a GMS could result in large amounts of funds being misdirected or taken from victims' bank accounts. GMS systems are key to the NGO funding ecosystem interruption to them would significantly interrupt our sectors operations. I have read Microsoft security blogs about Star Blizzard that showed phishing emails that referenced "grant making organizations" and targeted organizations like those in NGO-ISAC. These activities were attributed to the Star Blizzard Defendants. In my outreach to the Corporation I connected them with the threat analysts. Once I informed the Corporation, under information and belief, the Corporation began an investigation into the issue. **Figure 1** below is screenshot of the outreach I sent to the Corporation in connection with the phishing email. In the email below, "CCNY" is an abbreviation for the Carnegie Corporation of New York.



From: Ian Gottesman [redacted]
Sent: Thursday, April 27, 2023 11:14 AM
To: [redacted]
Subject: Re: CCNY fluxx portal question

Thanks [redacted] moving you both to BCC so you are not inundated with emails.

[redacted] it is nice to meet you. I was contacted by a threat analyst from Microsoft and [redacted] (an email security company) asking if an email from

Carnegie Corporation Fluxx <grants08-us-east-1-fluxxio[@]outlook.com>
Subject
Proposal Invitation to Carnegie Corporation of New York

Was legitimate and from us. It is obviously not from [redacted] and I assume not a legitimate email from CCNY Flux system. I would like to put you or someone from your IT or cybersecurity team in contact with the threat analysts. They should be able to help you get the outlook.com account shut down and also get the phishing emails removed and blocked from many systems.

If it is helpful we can also invite someone from CCNY to join the NGO ISAC a cybersecurity group that helps our sector with issues like this. I was contacted through that group because of Carnegie in the email address.

Please let me know what else I can do to help.

Thanks,

Figure 1

18. Spear phishing and phishing tactics like those deployed by Star Blizzard Defendants have required NGO-ISAC's member organizations to commit resources to their data and network security. Our member organizations have also turned to other organizations such as

Access Now for navigating the complexities of more serious incidents.

19. Access Now and the NGO ISAC have a partnership to work on complex cybersecurity issues. Both organizations focus on civil society actors and organizations that work in troublesome internet environments. Access Now and the NGO-ISAC have focused resources on Star Blizard victims who are both impersonated as part of these campaigns and targeted by these impersonations as part of spear phishing campaigns. Some of them are former U.S. Ambassadors who now work at NGOs on issues related to Russia, Ukraine, and the war there. When successful these spear phishing threats can lead to time consuming and costly remediation such as victims having to change bank accounts that were tied to compromised emails, struggling to get personal information removed from the internet, work with their network of peers to alert others to the issue, and create new email accounts. Even when these campaigns do not successfully breach accounts, they slow down victims' ability to work, eroding trust within the attacked communities, making their work harder and less effective. The NGO-ISAC and Access Now work with our network of NGO members, and civil society actors to rebuild their effective research and communication once they are targeted and attacked.

IV. CALL FOR LEGAL ACTION

20. Given the severe implications of the Star Blizzard Defendants' campaign, I strongly support the application for an emergency temporary restraining order and preliminary injunction. Such legal action is crucial to disrupting the operations of Star Blizzard and safeguarding NGOs from further cyberattacks.

21. The Court's swift and decisive action is necessary to address the threats posed by the Star Blizzard Defendants, ensuring that NGOs can continue their vital work without the constant risk of cyber intrusions and data breaches.

22. As a result of the acts of Star Blizzard Defendants, NGO-ISAC's member organizations have experienced harm to their brand and reputation. Given the amount of publicity that attacks on nonprofits and NGOs receive, this reputational harm is significant. Additionally, member organizations that are victims of attack face a loss of goodwill – members of the public may incorrectly attribute the attack to the member organizations – rather than attributing the harms to the Star Blizzard Defendants who are deploying these spear-phishing attacks.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Ian Gottesman

Cybersecurity Leader

Building a community of practice to improve cybersecurity for the nonprofit sector which employs 16%

- **Visionary Cybersecurity Leader** manages a diverse community of non-profits members, cybersecurity company partners, and organization friends to improve cybersecurity for the sector.
- Worked with NGO ISAC partners and members to find a 0-day 0-touch apple exploit being used by commercial malware vendors. The resulting patch was sent to **over 1 billion devices**.
- **Managed IT operations at multiple large international nonprofits**. Directed large IT projects such as upgrades for moving to a new building for all 300+ staff.
- **Conference speaker on cybersecurity** of nonprofits
- Founding Board Member of nonprofit group dedicated to advancing cybersecurity within nonprofit sector

Areas of Expertise/Signature Strengths

Cybersecurity | Incident Response | Cyber Strategy | Program Development | IT Infrastructure | Vendor Oversight | Cloud and Mobile Services | Integrated Digital Systems | Websites | Telecommunications | CRMs | Team Leadership | Budgets | Metrics

Professional Experience

NGO-ISAC | Washington, DC | April 2024-Current
Startup nonprofit building a community to secure our sector |

Chief Executive Officer | Selected as first hire and first CEO of NGO-ISAC. Worked with board and president on multimillion dollar fundraising campaign to enable hiring of 4 staff:

- **Hired staff** for startup NGO.
- Created weekly webinars for 200+ NGO members. Hosted annual conference for 150 member attendees with speakers from USG, leading cybersecurity vendors, and
- Grew paid membership by 300%
- Created programming to improve cybersecurity of our sector by using low cost or no cost solutions to improve
    - Created Cyber Car Wash for democracy NGOs to provide assessment and improvements for their cybersecurity using solutions from other NPOs, donated tools from vendors like MS, Okta, Cloudflare, and others to protect this sector before election.
    - Worked with other ISACs to create customized communication for our members.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE | Washington, DC | 2020–April 2024
Global nonprofit with 4 international centers providing strategic insight that advance international peace. $ 45M budget | 300+ staff

Chief Information Officer | Migrated traditional on prem IT infrastructure to cloud-based, mobile first environment. Recruited to lead an international IT team of 6 staff and 4 MSPs across 5 sites; manage $2.5M budget. Boosted fundraising, mass email outreach, and event management efforts through upgrade to Salesforce Non-Profit Success Pack. Highlights:

- **Within 2 weeks of hire, successfully executed mobile and cloud-based work from home initiative** for 300+ staff with no disruption of work, resulting in fully functional office on first day of work-from-office environment.
    - Migrated phones, file server, intranet, and other tools to the cloud; transitioned staff from desktop computers to laptops and trained on WFH programs, including Teams, Zoom, SharePoint and One Drive.
- **Reduced ongoing cybersecurity threats** to organization's communication and research efforts. **Secured $90K in grants** from Microsoft, YubiKey and others to upgrade software to better match new cloud first, mobile first environment; hired new director of cybersecurity; and created tools to train staff on cybersecurity.

WOMEN FOR WOMEN INTERNATIONAL | Washington, DC | 2018–2020

Global NGO that annually trains and empowers 20K women living in 6 post-conflict reconstruction zones. $25M budget | 250+ staff

Director, Global Business Solutions | Modernized IT technology and upgraded CRM to take organization's fundraising and communications to next level. Managed staff of 8 and $1.5M budget. Gained buy-in for upgrades across teams in the US and 6 countries. Trained IT staff on project management, business analysis, and to complete CRM implementation of projects, including online fundraising tool and GDPR compliance, upon departure. Highlights:

- **Overhauled and increased outreach and fundraising performance, efficiency, and donor payment security** by migrating from home-grown tools to industry-leading, cost-effective CRM. Led to $50K savings in licensing costs, reduced risk for credit card fraud, real-time, accurate constituent data and eased integration with cloud-based tools.
- **Cut costs and created unified global IT infrastructure** to ensure reliable computer service across global offices by standardizing IT purchases and selecting laptop vendor specializing in global NGOs, saving 30% in costs per computer.
- **Garnered agreement between US and international staff to select and adopt more efficient cloud-based budget tool** to more thoroughly track and report on increased grant-based and individual donor funds.
- **Contributed to building more cohesive and skilled global IT team by leading worldwide IT conference in Rwanda** to solve team IT challenges. Led to hiring global manager in Nigeria to train and provide resources for global IT staff and greater global team involvement in enterprise-wide decision-making.

CSIS: CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES | Washington, DC | 2007–2018

Bipartisan think tank that develops foreign and defense policy solutions for federal government. $ 45M budget | 350+ staff

Chief Information Officer | Web Director | Directed team of 12 and $2M budget to direct enterprise-wide information communications technology (ICT), web, and audiovisual tools and to manage security related to advanced persistent threats (APT). Trained staff on technology and security precautions**.** Promoted from web director in 2012. Highlights:

- **As CIO, orchestrated move to and $2.5M IT infrastructure upgrade** for new $100M LEED headquarters, including VOIP, data center, building security, AV, computers, and DAS (Distributed Antennae System).
  - **Upgrades boosted network security** and increased network speed **10-fold** and storage **15X.**
  - Provided hybrid on premise data center with cloud backup, and **under 4-hour disaster recovery**.
  - **Executed weekend move of 300+ staff to new HQ on time and without service interruption.**
- **As web director, overhauled web operations and implemented cutting-edge digital tools**, including upgraded CRM, podcasts, and videos to attract new viewers, doubling audience.
  - **Created iTunes U site,** establishing CSIS as sole think tank educational content provider.
  - **Founded innovative multimedia studio to deliver think tank's most important research** and to create online convening space for CSIS scholars and other experts, saving $300K annually.

Early Programming and Web Career includes positions with iBelong Networks; Youth Service America; New Horizons for Primary Schools, U.S. Peace Corps Jamaica; and Florida State University and University of Florida Faculty Group Practice. Highlights:

- **YOUTH SERVICE AMERICA**: **Set up first successful social media campaign** to expand YSA's online networks of volunteer photographers; Implemented new online messaging, advocacy, and CRM systems**; Implemented first-ever web analytics** to improved site effectiveness, helping to double tool download over previous]s year.
- **U.S. PEACE CORPS JAMAICA**: **Selected as Peace Corps volunteer for USAID project training teachers in technology in Jamaica.** Developed and maintained New Horizons for Primary Schools' website; Trained 1,200+ educators on technology tools; **Taught 7 technology modules, leading to a 55% increase in technology use in classroom.**
- **FLORIDA STATE UNIVERSITY**: Received Multiple Davis Website Productivity Awards as part of website redesigns.

Industry Leadership and Community Service

- **Current/Founding Board Member** | NGO Information Sharing and Analysis Centers (ISAC)| 2016–current
- **Conference Organizer/Speaker** | CIO4GOOD | April 2022 and April 2023
- **Panelist/Speaker**, Nonprofit IT Roundtable | ENABLING TECHNOLOGY | January 2021
- **Member,** DEI Taskforce | CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE | 2020-Current
- **CSIS Capital Region Corporate Champion Award Summer |** YEAR UP**|** 2017

Education

- **MPA**, Concentration: **Management and Information Sciences**, THE FLORIDA STATE UNIVERSITY, Tallahassee, FL
- **BA, International Affairs,** THE GEORGE WASHINGTON UNIVERSITY, Washington, DC

2024 CYBER THREATS TO NGOS

CYBER THREAT ALLIANCE

POWERED BY THE CTA

The Cyber Threat Alliance (CTA) is the industry's first formally organized group of cybersecurity practitioners who work together in good faith to share threat information and improve global defenses against cyber adversaries. CTA facilitates the sharing of cyber threat intelligence to improve defenses, advance the security of critical infrastructure, and increase the security, integrity, and availability of IT systems.

We take a three-pronged approach to this mission:

1. Protect End-Users: Our automated platform empowers members to share, validate, and deploy actionable threat intelligence to their customers in near-real-time.

2. Disrupt Malicious Actors: We share threat intelligence to reduce the effectiveness of malicious actors' tools and infrastructure.

3. Elevate Overall Security: We share intelligence to improve our members' abilities to respond to cyber incidents and increase end-user's resilience.

CTA is continuing to grow globally, enriching both the quantity and quality of the information shared among its membership. CTA is actively recruiting additional cybersecurity providers to enhance our information sharing and operation collaboration to enable a more secure future for all.

For more information about the Cyber Threat Alliance, please visit: https://cyberthreatalliance.org.

Cover Image produced by Lars Conard

CYBER THREATS TO NGOS WORKING COMMITTEE MEMBERS

Cisco Talos
Nick Biasini

CyberPeace Institute
Adrien Ogee
Alexandru Lazar
Stéphane Duguin

Defending Digital Campaigns

Fortinet
Val Saengphaibul

Granitt
Runa Sandvik

NetHope
James Eaton-Lee
Dianna Langley

NGO-ISAC
Ben Johnson
Frank McGothigan

Rapid7
Martin McKeay

RoundTable
Karim Beldjilali

Symantec by Broadcom
Scott Swett
Brian Ewell

Unit 42 Palo Alto Networks
Amer Elsad

UC Berkeley Center for Long-Term Cybersecurity (CLTC)
Sarah Powazek

Cyber Threat Alliance
Chelsea Conard
Michael Daniel
Jeannette Jarvis
Linda Beverly
Kate Holseberg

TABLE OF CONTENTS

EXECUTIVE SUMMARY 5

INTRODUCTION 6

CYBER THREATS TO NGOS 6

- The Challenge 6
- Threat Actors 7
- Intrusion Methods 7

PAIN POINTS FROM THREAT TYPES 7

- Pain Point: Stealing Money 7
- Pain Point: Espionage 9
- Pain Point: Disinformation 10
- Pain Point: Disrupting Operations 10

IMPROVING CYBERSECURITY: A PRACTICAL GUIDE 11

- The Cybersecurity Fundamentals 12
- Adopt a Management Framework 14

EXECUTIVE LEADERSHIP AND BOARD RESPONSBILITIES IN NGO CYBERSECURITY 15

- Board versus Executives: What's the Difference? 16
- Board-Executive Interaction 16
- Making Risk Decisions 16
- Approving Budget Allocations 17

WORKS CITED 18

MORE INFORMATION AND RESOURCES 19

EXECUTIVE SUMMARY

"Good cybersecurity is a team sport. Nonprofits need the strong support of the public and private sectors so they can safely and consistently continue to serve the parts of the planet and people who need it most."

— Dianna Langley, NetHope

Cyber threats affect everyone, but the nature of those threats and the resources to address them vary widely between organizations. Non-governmental organizations (NGOs) occupy a challenging place along this continuum because they face an array of significant threats, and have limited resources to counter this activity.

Given these challenges, the Cyber Threat Alliance (CTA) organized a coalition of industry leaders to focus on cybersecurity for NGOs. This Joint Analytic Report (JAR) outlines prevalent threats, suggests remediation strategies, and provides guidance for the executive leadership to enhance their nonprofit's cybersecurity posture. Aimed at empowering NGOs, this report is designed to equip organizations with an understanding of prevalent cyber dangers and to arm them with effective countermeasures.

Recommendations for NGOs:

1. **Emphasize Preparedness and Security Fundamentals:** NGOs must prioritize cybersecurity readiness; apply two-factor authentication (2FA), update software, and make regular backups as basic standards of security.

2. **Adopt a Comprehensive Cybersecurity Strategy:** A robust framework includes adopting and maintaining general cybersecurity policies and response plans, as well as contracting a Managed Security Service Provider (MSSP).

3. **Executive Responsibilities:** Leadership plays a pivotal role to navigate the cybersecurity landscape. A concerted effort from the boardroom to the frontline employees is essential to ensure the NGO's mission and operational integrity are safeguarded against cyber threats.

4. **Leverage Free and Accessible Resources:** Numerous free resources are highlighted in the CTA website Recommended Resources to aid NGOs to enhance their cybersecurity posture, including tools for phishing training, tabletop exercises (TTXs), and comprehensive guides from entities like NetHope, CyberPeace Builders, and NGO-ISAC.

This JAR serves as a call to action, urging NGOs and the cybersecurity industry to address cybersecurity challenges head-on. By fostering a culture of proactive cybersecurity management, NGOs can significantly enhance their resilience against cyber threats. This collaborative approach not only secures critical data and resources, but also ensures the continuity of vital missions in the face of evolving digital risks.

INTRODUCTION

Non-governmental organizations (NGOs) undertake a wide range of activities, working to address various social, environmental, and humanitarian concerns. They play a crucial role in complementing the efforts of governments and other stakeholders to address various challenges around the world. Every day, NGOs battle cyber actors seeking to perform reconnaissance, harvest stolen credentials and data, steal money, jeopardize the NGO's mission, and damage their reputation, to name a few. NGOs' cybersecurity capabilities to defend against their adversaries can vary due to the size, maturity, and resources to their organizations.

NGOs face many of the same cyber threats plaguing other industries, but they struggle to adequately fund or resource their cybersecurity needs. Numerous organizations have minimal budgets but large, distributed networks serving vulnerable populations. This mismatch contributes to them being attractive targets to threat actors including nation-states and hacktivists.

The resource limitations are a significant concern not just at the individual organization level, but across the entire NGO sector. Despite these challenges, NGOs have the opportunity to prioritize cybersecurity investments to protect their missions' successes. By shifting their perspective, NGOs can move away from viewing cybersecurity as a "technical luxury beyond our means" to recognizing it as "a critical enabler for achieving our goals."

Fortunately, enhancing security does not always come with a hefty price tag. Many measures focus on establishing effective processes and policies rather than high-tech solutions. As a result, NGOs can notably boost their cybersecurity without incurring substantial costs.

This report is an educational tool for NGOs, designed to elevate NGOs' awareness of cyber threats, offer remediation strategies, and assist in advocating leadership to invest in cybersecurity. It serves as a catalyst for cultural transformation within organizations, showcasing how NGOs can effectively evolve their cybersecurity posture. This comprehensive resource is a testament to the unique collaboration among industry leaders, notably CTA members working with entities like NetHope, the CyberPeace Institute, and the NGO-ISAC to build data-informed guidance and best practices that reflect the current landscape and the specific needs of NGOs. Through this collective effort, CTA aims to equip NGOs with tools to strengthen their cybersecurity practices, ensuring their crucial missions proceed with enhanced security and resilience.

Addressing these challenges requires collaboration from cybersecurity practitioners and NGOs. By enhancing the support framework dedicated to cybersecurity for NGOs, we can more effectively empower organizations to navigate the intricate landscape of cyber threats. In turn, strengthening their capacity to protect their essential work and a more robust defense of their missions.

CYBER THREATS TO NGOS

THE CHALLENGE

NGOs are exposed to a wider and more complex range of cyber threats than many organizations due to their involvement in political, governmental, and humanitarian areas. Alongside common cybercriminal activities similar to those encountered by commercial and governmental entities, NGOs are also targeted by nation-states and hacktivists. This combination of threats makes their cybersecurity landscape particularly challenging, requiring heightened vigilance and robust defense strategies.

The challenging cybersecurity landscape for NGOs not only encompasses digital threats but, in some instances, extends beyond the digital realm and

affects NGO personnel or clients in multifaceted ways. The complexity of these threats necessitates a broader discussion on how NGOs can better protect their infrastructure, staff, and constituency. Understanding the complex nature of these threats is essential, particularly in light of NGOs' constrained budgets and finite resources.

NGOs also operate within a context of markedly tighter resource limitations than other sectors, leading to fiscal constraints that hamper organizations' ability to thoroughly monitor and protect their digital environments. These disparities in resource allocation hinder their implementation of vital security best practices and critical protocols.

THREAT ACTORS

Threat actors do not always target NGOs because they are NGOs. Many actors are purely opportunistic, looking for any vulnerable target rather than focusing on a specific industry. While these actors may not possess the same patience and skill as a nation-state, criminals nevertheless pose a significant risk to NGOs. Criminal actors operate much like any corporate entity, with structures and strategies in place to exploit vulnerabilities. They can disrupt operations and steal the money an NGO needs to achieve its goals.

Meanwhile, by operating in conflict zones or working on issues that some see as provocative, especially when advocating for social or political change, NGOs are also prime targets for nation-state threat actors and hacktivists. Many nation-states see NGOs as a threat, and they utilize open source and private tools as an effective means to spy on or harass NGO personnel, as well as hinder NGO activity. Hacktivists can also target NGOs because they perceive them as "enemies." Therefore, the sensitivity and specific nature of NGO operations render them susceptible to harassment or disruption through malicious cyber activity in a way that many other organizations do not experience.

Additionally, insider threats can pose a concern, involving individuals within an organization who have privileged access to critical systems and can inadvertently or maliciously compromise security.

INTRUSION METHODS

How do malicious actors gain access to an NGO's digital environment? They use the same tools and techniques as for any organization. The two primary methods of intrusion are (1) social engineering, which involves persuading a human to take an action to open a hole in an organization's security, and (2) exploitation of known vulnerabilities, which are holes or weaknesses in the hardware or software used by the organization. Despite the impression media stories might give, incidents involving exploitation of previously unknown vulnerabilities (often called "zero-days") represent only a small fraction of security breaches (CISA).

PAIN POINTS FROM THREAT TYPES

Cyber actors targeting NGOs use a wide range of tactics and techniques within the two broad methods cited above, each with its own unique implications and consequences. In the following section, we will explore the top cyber threats in detail, delineating the primary objective behind each category and highlight the vulnerability they exploit in NGO operations.

PAIN POINT: STEALING MONEY

By virtue of being connected to the internet, NGOs are vulnerable to one of the most common kinds of cyber threats – criminals trying to steal money. The most common techniques for stealing money involve variations of social engineering, including phishing, spear phishing, vishing, smishing, and business email compromise. Additional approaches include fake websites and the gift card scam.

Social Engineering

Social engineering threats exploit human psychology rather than technological vulnerabilities to gain unauthorized access to information or systems. Among the most common forms are phishing, spear phishing, smishing, and vishing. Phishing involves sending emails with malicious links or attachments under the guise of legitimate sources, targeting a broad audience without much personalization. In NetHope's soon to be published '2024 State of Humanitarian and Development Cybersecurity Report,'nearly 80% of survey respondents experienced phishing in the prior 12 months, making phishing the most common of any threat type to NGOs (NetHope). Spear phishing, a more targeted version of phishing, focuses on individual recipients or specific entities within an organization, deploying well-researched and highly credible threats that often lead to the deployment of malware. In the same '2024 State of Humanitarian and Development Cybersecurity Report,' NetHope's initial findings show that over 60% of survey respondents experienced spear phishing in the prior 12 months, making spear phishing the second most common of any threat type (NetHope). Smishing utilizes SMS text messages to trick recipients into revealing personal information by posing as reputable entities, exploiting the immediacy and personal nature of text messages. Vishing, or voice phishing, involves phone calls where the attacker impersonates a credible authority to solicit personal and financial information, leveraging direct conversation to create a unique pressure that encourages victims to comply without verification.

Business Email Compromise

Business Email Compromise (BEC) represents a significant threat to the financial stability of NGOs. The goal is to trick employees into making unauthorized money transfers or revealing sensitive information that can be used for financial gain. As the name implies, the threat comes through an email to an employee or staff member. BEC activity is usually highly tailored to the victim organization, with the attacker having done some degree of reconnaissance to deceive the recipient. For example, malicious actors will find out the names of leaders in the organization and their roles, so that they can pretend to be the CEO asking for money to be transferred.

Fake Websites

Criminals can also target an organization's customers or donors to steal money through fake websites. In this technique, criminals mimic legitimate platforms with a high degree of accuracy. They then use a technique called "search engine optimization" (SEO) to get the fake website to show up higher than the legitimate site in search results. Unsuspecting customers or donors can then be tricked into providing sensitive information or making unauthorized payments. In these cases, the money is diverted before it ever arrives at the donor's intended destination.

> *NGOs are often targets of specific BEC scams where cybercriminals exploit the trust and authority of key personnel within the organization. In the Gift Card Scam, perpetrators impersonate a high-ranking individual, like the CEO, and send urgent requests via email or text messages to key employees. The visuals associated with this scam might feature company logos, signature blocks, and language that closely resembles that of the purported official. Thus, the attacker may pose as the CEO, claiming to be in a meeting and urgently request $200 worth of gift cards for a client or employee reward. The sense of urgency and perceived authority of the sender may pressure recipients into complying with the request without questioning its legitimacy, resulting in financial loss for the organization.*

Each method leverages a blend of technological tools and psychological tricks to exploit the innate trust and habitual responses of individuals, often culminating in the theft of money from unsuspecting victims.

PAIN POINT: ESPIONAGE

Due to the nature of their work, NGOs are subject to nation-states wanting to spy on their activities. Governments may use the collected information for a variety of goals, including arresting NGO personnel, learning about an NGO's sources, clients, or recipients, tarnishing the NGO's reputation, and/or supporting disinformation campaigns or social engineering. While the aforementioned techniques to steal money can also be used for espionage, the most common way that nation-states spy on NGOs is through spyware.

A mobile phone or laptop is the most common device for spyware; however, malicious actors can use other devices as well. Such devices include the vast array of "things" that can now be connected to the Internet, from cameras to appliances to vehicles. Often referred to as the Internet of Things (IoT) devices, these items often contain vulnerabilities that are not commonly addressed, and/or they contain default settings that allow for unauthorized access and surveillance. Further, most organizations are unfamiliar with how many IoT devices are connected to their network and how they are accessible from anywhere on the Internet.

"The level of sophistication in spyware dwarfs the sophistication of other cybersecurity activities that we see."

— Nick Biasini, Cisco Talos

Spyware ranges from relatively straightforward surveilance tools that can capture keystrokes and browsing history, to highly advanced systems like Pegasus, which can covertly infiltrate smartphones to access messages, calls, and even activate cameras and microphones without the user's knowledge. This technological sophistication highlights the dual nature of spyware: it exists both as a commerical product available for legitimate security purposes and as a mercenary tool used for more clandestine activities.

Commercial Spyware

Commercial spyware often masquerades as legitimate software, available through common channels such as app stores. It is a type of malicious software designed to access and collect private information from users' devices without their knowledge. Spyware can be particularly dangerous for NGOs, as it can gather sensitive information that could compromise the security and privacy of the organization.

Mercenary Spyware

Mercenary spyware represents a more targeted and dangerous threat. While commercial spyware is usually disseminated through widespread channels, mercenary spyware is developed and deployed by entities with substantial resources, often for specific espionage purposes against high-value targets, including influential figures within NGOs.

> *It is important to note that spyware often occurs in the form of a threat to mobile devices due to the personal nature of the data stored on phones. The threat is more significant for organizations that use personal devices for work-related tasks. Threats targeting mobile platforms present a growing concern for NGOs as these devices become increasingly integral to daily operations and communication. Mobile devices are often perceived as a smaller surface to manipulate compared to traditional computers because they may receive less device management, making them attractive targets to cybercriminals.*
>
> *Signs of infiltration or mobile device compromise include the device overheating, rapid battery drain, and unusual app behavior. A spyware intrusion may start from seemingly innocuous sources, such as accessing an intentionally shortened link, which might be sent by contacts you recognize, whether genuine or spoofed.*

PAIN POINT: DISINFORMATION

"An organization's reputation is one of the top assets leaders will try to protect."

— Karim Beldjilali, RoundTable

An organization's reputation is directly linked to stakeholder trust. Without stakeholder trust, NGOs cannot achieve their mission. This relationship explains why an organization's reputation is one of the key assets leaders are tasked with protecting. It also explains why nation-states and hacktivists seeking to hinder an NGO's work try to attack its reputation. From a cybersecurity perspective, these malicious actors can employ disinformation campaigns to spread false information, tarnish reputations, and generate opposition to the NGO and its work. Social engineering techniques are often integrated into disinformation campaigns. The rise of artificial intelligence (AI) and "deepfakes" make this threat even more potent.

Disinformation Campaigns Coupled with Social Engineering

Disinformation campaigns coupled with social engineering tactics present a multifaceted threat to NGOs, leveraging psychological manipulation and deceptive techniques to exploit human vulnerabilities. These campaigns aim to spread false or misleading information, often with the goal of damaging an organization's reputation, sowing discord among stakeholders, or influencing public opinion. Malicious actors will masquerade as trusted sources and/or leveral emotional appeals to deceive individuals into divulging sensitive information or taking actions detrimental to an organization's interests.

AI and Deepfake Technology Influencing Disinformation

Although not yet widespread, emerging technologies such as artificial intelligence (AI) are poisted to heighten NGOs' financial vulnerabilities. These advanced tools enable fraudsters to craft highly convincing impersonations and manipulate digital content, posing a significant detection challenge. For instance, "deepfakes" - synthetic media in which a person in an existing image or video is replaced with someone else's likeness using AI - can be particularly damaging. Smaller NGOs might be targeted by localized fraud activity aimed at exploiting specific donor bases, while larger organizations face the risk of broader disinformation campaigns that could jeopardize major funding streams.

PAIN POINT: DISRUPTING OPERATIONS

Ransomware

Ransomware is a type of malicious software designed to block access to a computer system or files until a sum of money is paid. Ransomware typically encrypts the victim's files or locks the entire system down, rendering it unusable. The attackers then demand a ransom, usually in cryptocurrency, in exchange for providing the decryption key or restoring access to the system. Ransomware attacks can cause significant disruption to individuals, businesses, and organizations, often resulting in financial losses and data breaches.

While this type of attack may sound like it requires significant technical skills to execute, "ransomware-as-a-service" models have emerged over the past few years that enable unskilled actors to carry out such attacks. In this model, different groups work together to carry out ransomware, each specializing in a specific aspect; writing malicious code, gaining access to organizations, or encrypting data. Thereafter, each group receives a share of the eventual payments. The group collaboration enables criminal actors to increase the volume of ransomware, creating greater levels of disruption to organizations.

Notably for NGOs, they face ransomware that is politically motivated, where the threat is not always intended to obtain money, but rather to disrupt critical operations by sabotaging essential voting processes or compromising sensitive data associated

with high-profile events. To inhibit an organization, threat actors have a tactic to not always activate the ransomware immediately. The ransomware can be deployed months after the infiltration, where a threat actor will reside in the network after performing lateral movement, exacerbating the challenge of detection and mitigation.

"We see about one ransomware attack a month among our Members."

— James Eaton-Lee, NetHope

Ransomware has greater impact when malicious actors apply "double extortion" tactics. With this extension, actors not only encrypt the victim's data, but also steal and threaten to release the data publicly unless the ransom is paid. This dual-pronged approach amplifies the pressure on organizations to comply with the demands, adding complications of reputtional damage and regulatory scrutiny alongside the disrupted operations. For NGOs, such tactics pose significant threats, as the potential exposure of sensitive information can jeopardize their credibility and the safety of their staff and beneficiaries.

In certain cases, ransomware may escalate into "triple extortion" wherein attackers extend their targets beyond the organization to encompass its network of supporters and end-users. In the context of NGOs, however, this strategy may prove futile, as these entities and their beneficiaries often lack the financial means to meet ransom demands. Consequently, attackers may shift their focus to target those who finance NGOs, such as grant providers, by exploiting their ability to pay, escalating the ripple effect of the ransomware across the ecosystem.

NGOs who have been affected by ransomware are not shielded from future attacks. The same or other ransomware actors could target the NGO in the future. It is possible that during recovery effects, the original threat actor, or other actors, could have undetected access to a network, leading to a subsequent breach. This stark reality calls for a paradigm shift in how NGO leaders perceive post-attack security. It is imperative to abandon any false sense of safety and acknowledge that the first attack could be a precursor to a sustained campaign.

Denial of Service

Denial of Service (DoS) is a threat that can disrupt essential services and impede operations. DoS involves overwhelming a targeted system with a flood of network traffic, rendering it inaccessible to legitimate users. For NGOs, which often rely on digital platforms to deliver vital services and communicate with stakeholders, the threat of DoS can have significant consequences, with the potential to completely halt operations.

NGOs can also be an unwitting participant in a DoS. Threat actors could gain access to an NGO's IoT device and then make that device part of a "botnet." A botnet is a network of internet-connected devices, each of which has been infected with malware, allowing them to be controlled remotely by a malicious actor without the owner's knowledge. These botnets utilize the combined computing power of many devices to work together and generate the network traffic used in a DoS. When malicious actors use an organization's IoT devices for a DoS, the NGO's technology will reduce performance.

IMPROVING CYBERSECURITY: A PRACTICAL GUIDE

In the face of these threats, what should an NGO do? The good news is that, while no organization can reduce its cyber risk to zero, NGOs can substantially reduce their risk and enhance their ability to recover if they suffer a cyber incident. Further, these steps do not necessarily involve spending huge amounts of money, deploying lots of complex technology, or impeding workflow. Instead, to better safeguard their essential work, NGOs should start with what we call the cybersecurity fundamentals. These practices are

applicable to almost any organization and reduce your cyber risk, regardless of the threat actors your organization faces. Further, these steps are not all or nothing; even partial implementation will improve an organization's cybersecurity. Once an organization has the fundamentals in place, it can adopt a more comprehensive cybersecurity management framework and begin to implement more complex controls that protect against more sophisticated threats.

Between early 2022 and 2024, the CyberPeace Builders with the CyberPeace Institute conducted 148 General Cybersecurity Assessments, involving 108 distinct NGOs, to help nonprofits evaluate their own maturity level and compare to industry standards and peers.

The CyberPeace Builders is dedicated to strengthening the cybersecurity posture of NGOs by providing comprehensive assessments, guidance, and support to implement effective security measures. These evaluations revealed that certain controls significantly improved assessment scores.

Those controls are marked with a .

THE CYBERSECURITY FUNDAMENTALS

For entities just starting out on their cybersecurity journey, the following four actions will lay the foundation for more advanced work. These actions include:

1. Change the mindset
2. Manage cybersecurity proactively
3. Contract with a managed security service provider
4. Implement five key cybersecurity controls

Change the Mindset

The first fundamental is to stop treating cybersecurity as a technical luxury. Instead, NGOs should treat cybersecurity as a critical mission enabler to ensure that clients, customers, and recipients receive the appropriate services, that donors have confidence resources will reach intended recipients, and that staff are digitally protected. Adopting a different mindset for cybersecurity changes the way the entire organization engages with the topic for the better.

Manage Proactively

Once an organization thinks about cybersecurity as a mission enabler, then it needs to start managing it proactively. While this step will become more complex over time, at the beginning it consists of three parts:

1. Adopt general cybersecurity policies: Security policies are the backbone of an organization's cybersecurity framework, providing clear guidelines and procedures to protect sensitive information and technological assets. Fortunately, organizations do not have to create policies from scratch. Many generic versions are available that can be adapted to an organization's specific circumstances. Such resources are located on the CTA website.

2. Adopt response plans: At some point, every organization will have a cybersecurity incident, experience a natural disaster, or suffer some disruption in its operations. When such events happen, the organization needs to have plans in place for how to respond. These plans should include an Incident Response Plan, which outlines steps to take in response to a security breach; a Disaster Recovery Plan, detailing procedures for recovering lost data and restoring system functionality after a breach; and a Business Continuity Plan, ensuring that critical business functions can continue during and after a significant disruption. Even though no incident response or disaster recovery effort will

unfold exactly as planned, having a plan enables an organization to respond effectively. As with general cybersecurity policies, sample response plans exist for an NGO to adapt it to its particular circumstances.

3. Conduct regular oversight: Just like with adhering to accounting practices and managing legal liability, cybersecurity is a leadership responsibility. Therefore, NGO leaders should regularly ask questions, receive reports, and make changes as necessary to keep cybersecurity a management focus. Recently, more emphasis has been put on a Board of Directors for oversight of cybersecurity. In light of this trend, we have included the next section to discuss the relationship between executive leadership and the Board and their respective responsibilities.

These policy decisions are not always easy to implement consistently considering the unique operational model of NGOs, especially those that rely heavily on volunteers. The inconsistency in training and commitment levels, alongside the competitive cybersecurity talent market, presents notable challenges to establish effective cybersecurity practices. Nevertheless, overcoming these obstacles is worthwhile. Robust cybersecurity policies can significantly enhance an NGO's credibility, attract more donors, and ultimately contribute to its financial health and sustainability, despite the initial hurdles in talent acquisition and training.

Contract a Managed Security Service Provider (MSSP)

Few organizations have the ability to provide all of their cybersecurity in-house. With the exception of large enterprises, some portion of the cybersecurity work needs to be outsourced to an MSSP. An MSSP can provide key services, such as monitoring the "dark web" for leaked information about an organization and scanning the organization's website and applications for vulnerabilities . Further, an MSSP can provide firewall and filtering services and keep them up to date.

Implement Five Key Cybersecurity Controls

"NGOs need to set up basic standards of security to maintain their operations."

— Martin McKeay, Rapid7

The final step for entities starting out on their cybersecurity journey is to implement five key cybersecurity controls. Different expert groups recommend slightly different cybersecurity measures. The United Kingdom has the cybersecurity essentials, Australia has the essential eight, the Institute for Security and Technology's Blueprint for Ransomware Defense identifies 14 foundational controls, and the Center for Internet Security has its top 20, just as examples. However, five security controls stand out as having a high return on investment and show up in all of the sets above:

- Use a **password** manager: people often struggle to generate their own passwords. They may follow a personal algorithm to create a unique, new password; however, that password can potentially be guessed if previous passwords are known. Yet, asking people to remember long, random, and unique passwords is impossible without help. Password managers solve this struggle. A password manager enables a user to only memorize one complex, unique password. The tool then creates and maintains the passwords for websites and applications, enabling long, random, and unique passwords for each.

- Use more than a password: Referred to as two-factor **authentication** (2FA), the core idea is that the organization needs to use more than just a username and password to verify that someone trying to log in or access an account is who one says one is. Although any form of 2FA is better than none, using a trusted authenticator application rather than SMS for 2FA provides a more secure verification process. For NGOs operating in areas without reliable internet access, a physical security token, like a YubiKey,

offers a viable alternative by providing a tangible second factor of authentication, making accounts significantly harder to compromise. This control should apply to personal devices used to access NGO Information Technology (IT) systems.

- **Update** software automatically: Keeping all software up to date ensures that an organization employs all the latest patches. Since a key threat outside of social engineering is exploiting known vulnerabilities, having the latest software dramatically reduces cyber risk. Cybersecurity is an ongoing effort, and updates are important to help address vulnerabilities that have been uncovered, as well as to provide ongoing maintenance. Therefore, instead of trying to remember to check for updates or ignoring update notifications, enable automatic update installations whenever possible.

- Filter **links**: Make sure that your MSSP employs a tool to filter out as many malicious links as possible. Since social engineering usually involves malicious links, having the ability to filter out known bad links reduces risk. Of course, these filters will not catch all the malicious links, so users must remain wary, but filtering will help.

- Make regular **backups**: Although adversaries may try to corrupt backups or use extortion techniques that do not rely on encrypting data, having robust data backups in place greatly increases organizational resilience to a wide variety of threats. Backups can be done using cloud services or storage devices like external hard drives that are not normally connected to the network or other devices; storing data in an alternative location that is safe and secure provides another layer of protection.

A useful mnemonic for remembering these five controls is to think of them as your friend PAUL B: passwords, authentication, updates, links, and backups.

ADOPT A MANAGEMENT FRAMEWORK

Once an organization has the fundamentals in place, the challenge is maturing cybersecurity processes and establishing a culture that embraces security. How should an NGO prioritize tasks, assign responsibility, and allocate resources? In other words, it needs a management framework. Fortunately, resources exist to help with this challenge, such as the National Institutes of Standards and Technology's Cybersecurity Framework 2.0. The Framework is not a cookbook of technical controls; rather, it provides a way to think about cybersecurity at an executive level. Other frameworks can provide the necessary scaffolding to manage cybersecurity over the long-term. The one that works best for an organization will depend on its location, size, and resources. The key is to select a framework, implement it over time, and track progress against agreed upon goals. Within this broad range of activities, two are worth highlighting as advanced steps.

Security Awareness Training

Educating users about the dangers of opening or clicking a suspicious email attachment or link will not eliminate a threat, but it will demonstrably reduce the frequency with which it occurs. If users receive suspicious or unexpected messages from someone whom they know, users should directly contact the individual through a different channel to confirm the message (Abrougui). An unsolicited WhatsApp message from a sender whom one does not know is an example of a red flag.

To further equip organizations, leaders with security responsibilities can play a pivotal role by leading workshops focused on ransomware, helping to clarify the signs of an attack and developing strategic responses, including decisions around ransom payment. Such education is vital to prepare the entire organization – from the boardroom to the frontline employees – to recognize and respond to cybersecurity incidents promptly and effectively.

"Trust but verify by picking up the phone and calling the number after a lookup that it's a valid number to call. If you are suspicious of a message from an individual or organization whom you know, verify with them through a different channel. It is possible the legitimate phone number was spoofed."

— Ben Johnson, NGO-ISAC

Device Security

All users should maintain up-to-date devices to allow security updates to address potential vulnerabilities. Users should also reboot phones regularly as many spyware applications are designed to persist only until the device is restarted (Abrougui). To enhance device security further, running antivirus scans helps detect and remove any malware that could have slipped through. In extreme cases where a device is compromised, performing a factory reset stands as the most effective method to completely remove all traces of an infection, returning the device to a secure state.

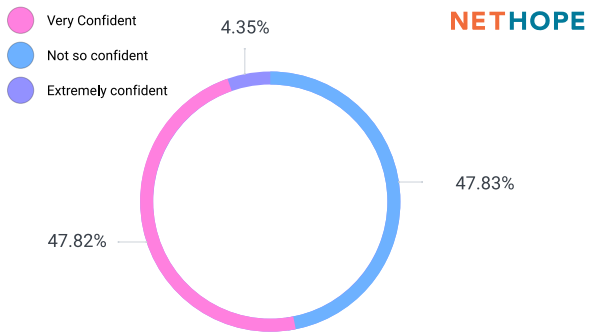
Organizations such as Access Now and Citizen Lab are valuable resources for navigating the complexities of spyware incidents. In the event of a mobile attack, immediate actions include consulting a threat researcher or contacting the State Department if the compromise occurs abroad. One may also place the phone in a secure bag and send it to experts like Citizen Lab for analysis. In this way, NGOs integrate physical security measures with digital safeguards to protect mobile devices and other physical assets.

EXECUTIVE LEADERSHIP AND BOARD RESPONSBILITIES IN NGO CYBERSECURITY

As noted in the previous section, executive leaders and the Board both play pivotal roles in cybersecurity. However, NGOs with less experience in managing cybersecurity may not be clear on what those roles are and how they differ. Therefore, this section outlines each role's key elements and describes how they complement each other.

NetHope's soon to be published '2024 State of Humanitarian and Development Cybersecurity Report' supports the notion the role of cybersecurity is not clear for many NGOs (NetHope). The survey reveals a distinct division among these organizations, with respondents nearly evenly split between those who are confident in their organization's cybersecurity visibility and management and those who are not.

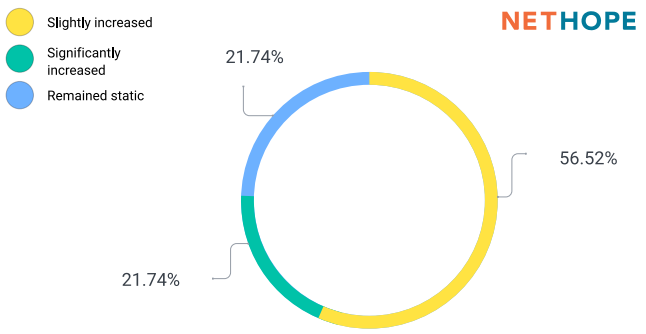
Are you confident that cybersecurity is a viable and well-managed risk for you?



On the other hand, this same survey indicates a positive trend in cybersecurity management. 78% of responding organizations reported an improvement in cybersecurity management over the last year, as shown in the next graphic (NetHope). Notably, there was no indication of a decline in cybersecurity quality among the surveyed organizations, implying

a sector-wide recognition of the critical nature of robust cybersecurity practices.

In the last 12 months, do you feel your organization's program in relation to your organization's needs has:



"The best way to avoid chaos is to have a culture of security and start early with conversations about how to best prepare for potential incidents."

— Runa Sandvik, Granitt

BOARD VERSUS EXECUTIVES: WHAT'S THE DIFFERENCE?

The key difference is straightforward to state, although sometimes difficult to implement in practice: Boards oversee cyber risk while executives manage cyber risk (Clinton). Thus, the Board's duty is to ask the right questions, approve the overall level of risk the organization is willing to take on, and hold executives accountable for implementing necessary cybersecurity measures. Boards should not choose cybersecurity solutions or direct specific actions (Clinton).

"Speaking to the C-Suite is one of the best ways to impact cybersecurity."

— Karim Beldjilali, RoundTable

In contrast, executives should provide the Board with a cyber risk assessment, explain how cybersecurity can support the organization's mission, identify and track appropriate cyber metrics, allocate adequate resources, and implement the cybersecurity measures provided earlier in this report.

BOARD-EXECUTIVE INTERACTION

In the for-profit world, and particularly for public companies, there is an ongoing debate about the "right" way for Boards and executives, particularly Chief Information Security Officers (CISOs), to interact. For most NGOs, the specific mode of interaction is less important than the fact that it occurs at all. For example, smaller NGOs might lack a dedicated CISO, and so cybersecurity responsibilities might fall to another executive. Some larger NGOs may choose to have the CISO report directly to the Board, while others might have the CISO report through the executive responsible for overall risk. The key is ensuring that the Board receives the necessary information to make risk-informed decisions and approve budget allocations.

MAKING RISK DECISIONS

Regardless of size, the necessity for leadership to have candid discussions about risk acceptance is critical. The Board and executives must understand that choosing not to implement certain cybersecurity measures equates to accepting a certain level of risk. Integrating cybersecurity risk into the organization's overall risk calculus is essential. This integration helps it become an integral part of business continuity plans focused on security and vital business operations.

To enable these risk conversations, decisions must be framed in clear, jargon-free language, to ensure all organizational leaders and Board members are considering the same problem and potential actions. A human-centered dialogue around cybersecurity fosters engagement and facilitates comprehension of its fiduciary impacts. Simplification of the topic through clear policies and educational initiatives can demystify cybersecurity, transitioning NGOs from a state of reactive measures to a proactive stance.

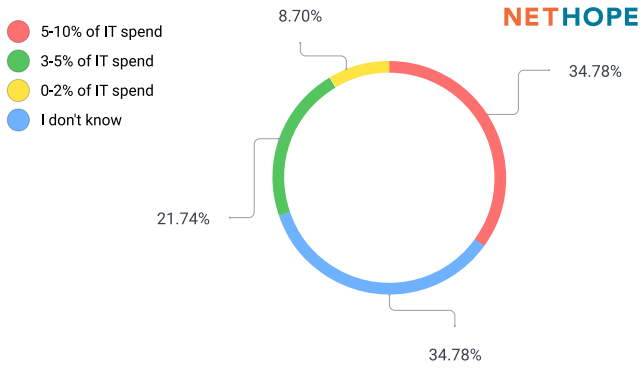
"Running an entity that is cyber secure is more profitable than running organization that is not."

— Stéphane Duguin, CEO, CyberPeace Institute

APPROVING BUDGET ALLOCATIONS

Once a Board accepts a certain level of cyber risk, executives have to allocate adequate resources to achieve that targeted level. While the specific amount required will differ between organizations, the graph below from NetHope's soon to be published '2024 State of Humanitarian and Development Cybersecurity Report' illustrates the current cybersecurity budget allocations among various organizations. Currently, the majority of organizations invest between 3% to 10% of their IT budget on cybersecurity measures (NetHope). The "right" allocation is the one that allows the organization to accept its desired level of risk.

What is your cybersecurity budget?



WORKS CITED

Abrougui, A. Global Trends in Digital Security. Internews, Nov. 2023, internews.org/wp-content/uploads/2023/11/Global-Trends-in-Digital-Security.pdf.

Clinton, Larry. *Cybersecurity for Business: Organization-Wide Strategies to Ensure Cyber Risk Is Not Just an IT Issue*. Kogan Page, 2022.

CISA, Cybersecurity Advisory AA23-215A: Cybersecurity and Infrastructure Security Agency. “AA23-215A: Cybersecurity Advisory.” CISA, 3 Aug. 2023, www.cisa.gov/news-events/cybersecurity-advisories/aa23-215a.

NetHope. “NetHope.” NetHope, 2024, www.nethope.org. (NetHope, 2024 State of Humanitarian and Development Cybersecurity Report)

MORE INFORMATION AND RESOURCES

For more information and resources, visit the CTA website.

CYBER THREATS TO NGOS
2024

CYBER THREAT ALLIANCE

POWERED BY THE CTA

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Microsoft Corporation, a Washington State Corporation, NGO-ISAC, a New York State Non-Profit Organization, Plaintiffs, v. John Does 1-2, Controlling A Computer Network and Thereby Injuring Plaintiff and Its Customers, Defendants.	Civil Action No. **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5.1**

DECLARATION OF YOTARO SHERMAN IN SUPPORT OF APPLICATION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, Yotaro Sherman, declare as follows:

1. I am the Associate Director of Information Technology (IT) of the Carnegie Corporation of New York ("Corporation"). I make this declaration in support of Plaintiffs' Application for an Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause re Preliminary Injunction. I make this declaration of my own personal knowledge or on information and belief where noted. If called as a witness, I could and would testify to the truth of the matters set forth herein.

2. I have been employed by the Corporation since 2009. In my role at the Corporation, I manage the organization's cybersecurity initiatives, technology architecture, security software and monitoring, incident response planning, policies, procedures and staff training/awareness. In this role, my responsibilities include the internal investigation of reports associated with a variety of IT issues impacting the Corporation, its employees, and associated partners. This includes

investigating reports of phishing or spear phishing emails.

3. I am also responsible for coordinating complex technology systems, facilitating development and maintenance of internal- and external-facing applications, and directing IT projects to meet business objectives, operational goals and key business priorities. Prior to joining the Corporation, I served as the Director of Information Technology at an organization that was an independent entertainment distributor and collector of independent digital content. A current version of my curriculum vitae is attached to this declaration as **Exhibit 1.**

I. CARNEGIE CORPORATION OF NEW YORK

4. The Carnegie Corporation of New York is an NGO-ISAC member organization, and one of America's oldest grantmaking foundations. It was established by Andrew Carnegie in 1911 "to promote the advancement and diffusion of knowledge and understanding," is one of the oldest, largest and most influential of American foundations. Some notable contributions of the Corporation include: (i) expansion of higher education and adult education, (ii) advancement of research on learning and cognitive development in early childhood, (iii) promotion of educational and public interest broadcasting, (iv) advancement of minorities and women in precollege and higher education, (v) heightening public understanding of the education and health needs of children and adolescents, (vi) investigation of risks of superpower confrontation, nuclear war, and ethnic and civil strife. Today, the Corporation promotes the advancement and diffusion of knowledge and understanding. In keeping with this mandate, the Corporation's work focuses on the issues of international peace,[1] the advancement of education and knowledge, and democracy.

[1] The Corporation's grant program on International Peace and Security focuses on global issues, including Russia. In 2022, the Corporation issued a report analyzing how Russia's invasion of Ukraine has adversely affected US-based Russian Studies efforts. Wilfred Chan, *How Russian Studies Is Grappling with the War in Ukraine*, Carnegie Corporation of New York, available at https://www.carnegie.org/our-work/article/how-russian-studies-is-grappling-with-the-war-in-ukraine/ (May 3, 2024).

5. The Corporation has helped establish or endowed a variety of institutions, including the Carnegie libraries, the National Research Council, the Russian Research Center at Harvard, and the Children's Television Workshop, and for many years heavily supported Carnegie's other philanthropic organizations, especially Carnegie Endowment for International Peace (CEIP), the Carnegie Foundation for the Advancement of Teaching (CFAT), and the Carnegie Institution of Washington (CIW). It has funded the writing of books and studies, as well as the organization of conferences and international exchanges, radio shows, legal proceedings and other activities. Through its activities, the Corporation has had a great impact on the information and knowledge available to citizens and government alike. Its work and that of its grantees has exerted a substantial influence on public discourse and policy.

II. OVERVIEW OF THE STAR BLIZZARD THREAT

6. My declaration concerns the spear-phishing attacks targeting nonprofits and NGOs, and as it applies here, regarding the Star Blizzard phishing operation. *See* Declaration of Sean Ensz in Support of Plaintiffs' Application For An Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("Ensz Decl.") ¶ 1. Star Blizzard Defendants are believed to be a Russia-based operation that engages in spear phishing resulting in the online impersonation of individuals and organizations, the infiltration of email accounts, and the exfiltration of sensitive and confidential information from those online accounts. Complaint ¶ 3. Star Blizzard Defendants are formerly known as SEABORGIUM and also known in the cybersecurity community as the Callisto Group, COLDRIVER, and BlueCharlie.

7. According to Microsoft's investigations, the Star Blizzard Defendants' campaigns target over 30 organizations, in addition to personal accounts of people of interest. Star Blizzard Defendants primarily target NATO countries, particularly the United States and the United

Kingdom, and other countries in the Baltics, the Nordics, and Eastern Europe. Complaint ¶ 18.

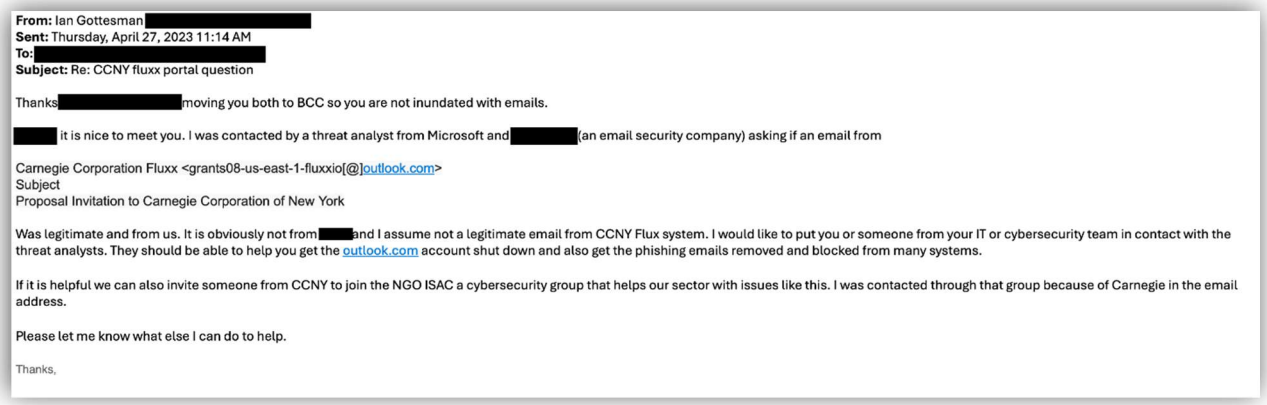
8. Microsoft has observed the Star Blizzard Defendants' campaigns continue to target NGOs, think tanks, government employees, and personal accounts belonging to current and former military and intelligence officials and policy advisors. The individuals targeted by these attacks predominately reside in the U.S., in and around the Washington, D.C. area. Complaint ¶ 14.

III. IMPACT ON THE CORPORATION

9. As discussed earlier, the Corporation's promotes the advancement and diffusion of knowledge and understanding around the issues related to international peace, the advancement of education and knowledge, and democracy. It has done so by establishing a grant program that provides financial support to applicants whose projects are focused on these areas. Once the Corporation issues a grant, the grant recipient (also called a grantee) is issued a grant number. This grant number is not public information. The grantee has a shared responsibility with the Corporation to manage the projects and its finances responsibly. As part of this process, a grantee is required to submit a report about the project's finances and status. The Corporation uses a grant management software called Fluxx and one of its features is the ability for grantees to submit reports through Fluxx's online portal associated with the Corporation's Fluxx account.

10. The Corporation and its grantees have been targeted by Star Blizzard Defendants by impersonating the Corporation in spear phishing emails to grantees. The Corporation was first made aware of Star Blizzard Defendants' spear phishing operation by Ian Gottesman, the current Chief Executive Officer of the NGO Information Sharing and Analysis Center ("NGO-ISAC"), who was at that time, with the Carnegie Endowment for International Peace ("CEIP"). **Figure 1** below is an email from Mr. Gottesman detailing the fake email and efforts by a threat analyst from the Microsoft Corporation ("Microsoft") in investigating the authenticity of an email purportedly

sent by the Corporation.



From: Ian Gottesman [redacted]
Sent: Thursday, April 27, 2023 11:14 AM
To: [redacted]
Subject: Re: CCNY fluxx portal question

Thanks [redacted] moving you both to BCC so you are not inundated with emails.

[redacted] it is nice to meet you. I was contacted by a threat analyst from Microsoft and [redacted] (an email security company) asking if an email from

Carnegie Corporation Fluxx <grants08-us-east-1-fluxxio[@]outlook.com>
Subject
Proposal Invitation to Carnegie Corporation of New York

Was legitimate and from us. It is obviously not from [redacted] and I assume not a legitimate email from CCNY Flux system. I would like to put you or someone from your IT or cybersecurity team in contact with the threat analysts. They should be able to help you get the outlook.com account shut down and also get the phishing emails removed and blocked from many systems.

If it is helpful we can also invite someone from CCNY to join the NGO ISAC a cybersecurity group that helps our sector with issues like this. I was contacted through that group because of Carnegie in the email address.

Please let me know what else I can do to help.

Thanks,

Figure 1.

11. As part of our investigation into the issues, our team was also made aware of a blog Microsoft issued around Star Blizzard Defendants' activities that impersonated the Fluxx grant management system. **Figure 2** below is the Star Blizzard Defendants' phishing email example in the blog – it referenced that a "report is overdue" and purportedly comes from the Fluxx grant system.

Date: Thu, 18 May 2023 11:21:46 +0000
From: [redacted]
Return-Path: grants07us-east@fluxx-east.com
To: [redacted]
Message-ID:
<CABjCnfCX=j=rc5pdBqGJcCBZnw+8DChjAuO_5Fcuizr34fMZ5g@mail.gmail.com>
Subject: Report Overdue - [redacted]

Figure 2.

12. Since the Corporation uses the Fluxx grant management system, the Corporation issued a notice to all 2,600 grantee contacts of the Corporation's active grants to alert them of potential spear phishing attempts. Grantees began reporting receiving emails with the same identifying features, which they initially believed to be a legitimate communication from the Corporation. True and correct snapshots of these phishing emails are included with this declaration as **Exhibit 2** (identifying information contained within the Images included in the Exhibit have been redacted for privacy of the targets and victims of the Star Blizzard Defendants). Among those who reported receiving the Star Blizzard Defendants' spear phishing emails are grantees at universities as seen in **Images 1 – 3** in Exhibit 2 attached to this declaration.

13. The Corporation investigated the spear phishing reports and found that Star Blizzard Defendants' spear phishing emails to the Corporation's grantees impersonated the Corporation's grant program, referenced that reports were overdue, identified the need for a Fluxx grant portal submission, and even referenced grant numbers associated with the issued grants. A link to log into the Fluxx report submission system was included in the spear phishing emails. An examination of the sender email addresses in the reported phishing emails showed that they were not issued by the authentic email address associated with the Corporation's Fluxx grant system. The Star Blizzard Defendants also used the Corporation's trademarked name "Carnegie Corporation of New York" on the subject line of their malicious emails. In the examples shown in Exhibit 2, Star Blizzard Defendants referenced the correct grant numbers for two of the grantee victims and referenced two incorrect grant numbers for the other two grantee victims. *See* **Appendix C** to the Complaint for the Corporation's trademarks.

14. The Star Blizzard Defendants, by referencing specific features like a grant number and a real document type, demonstrates that the Star Blizzard Defendants had access to and were

able to view non-public information in its victim's accounts. Given this level of specificity, the Corporation is harmed because grantee victims are tricked into believing the legitimacy of the email and will be more likely to engage with the lure that the Star Blizzard Defendants include in the spear phishing email. Since two of the four spear phishing emails referenced incorrect grant numbers, the Star Blizzard Defendants likely only had access to information in their target's emails and not the Corporation's secured, internal grant management system or any other of the Corporation's internal systems.

15. The Corporation invested a significant amount of resources and time in order to mitigate the risks that Star Blizzard Defendants posed and additionally, to strengthen the Corporation's data security and IT system totaling approximately $200,000 since 2023. My team spent over forty hours to investigate the Star Blizzard Defendants' spear phishing activities (which included outreach to the Corporation's 2,600 grantee contacts), engaged Fluxx to assess the grant management system, engaged an outside firm to conduct a risk assessment, and then committed additional resources and time to implement additional security recommendations to protect the Corporation, its grantees, and other partners from the Star Blizzard Defendants' activities. Since the grantees rely on the Corporation for funding the important work they do to advance the knowledge and understanding around the issues related to international peace, the advancement of education and knowledge, and democracy, any diversion of the Corporation's resources and time has a direct impact on achieving the Corporation's mission and a grantee's work.

16. The Star Blizzard Defendants' activities irreparably harm the Corporation by damaging its reputation, brand, and goodwill cultivated with its grantees and organizational partners. The spear phishing attacks that the Star Blizzard Defendants perpetrated against the Corporation's grantees are incorrectly attributing their activities to the Corporation. To be an

effective partner within the nonprofit and non-governmental affairs community, the Corporation must be seen as a trusted organization by its grantees and organizational partners. The Corporation has invested significant resources and time to establish itself, its brand, and develop relationships over time both domestically and internationally, and are determined to ensure that its reputation remains intact.

IV. CALL FOR LEGAL ACTION

17. Given the severe implications of the Star Blizzard Defendants' campaign, I strongly support the application for an emergency temporary restraining order and preliminary injunction. Such legal action is crucial to disrupting the Star Blizzard Defendants' spear phishing operations and safeguarding the Corporation, its grantees, and its partners. Without the Court's intervention, the Corporation, its grantees, and its partners will continue to suffer from harm caused by the Star Blizzard Defendants' actions.

18. The Court's swift and decisive action is necessary to address the threats posed by the Star Blizzard Defendants, ensuring that the Corporation can continue its vital work to support work advancing international peace, education and knowledge, and democracy.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge. Executed on September 24, 2024 in New York, New York.

/

_____

Yotaro Sherman

Associate Director of Information Technology
Carnegie Corporation of New York

Yotaro Sherman

PROFESSIONAL EXPERIENCE

Carnegie Corporation of New York **2009 – Present**

Associate Director of Information Technology *2016 – Present*
Business Application Delivery Manager *2009 – 2016*

Roles and Responsibilities

- Directly oversees the department's business application support. This includes identifying and implementing enhancements, performing upgrades, developing reports and interfaces, servicing end user requests, addressing any issues and managing vendor relationships.
- Researches, analyzes, documents, designs, and implements improvements and additions to existing workflow procedures. Promotes the use of data analysis/management tools throughout the organization.
- Manages Carnegie Corporation's cloud-based infrastructure. Monitors ongoing resource requirements, conducts application and data migrations, performs problem resolution and proposes the adoption of new tools and services.
- Provides significant contributions to the organization's cybersecurity mandates, encompassing our technology architecture, security software and monitoring, incident response planning, policies, procedures and staff training/awareness.
- Partners with all departments on adopting innovative ways technology can improve the delivery of Carnegie's mission and goals. Develops and deploys metrics to inform business decisions.
- Conducts vendor evaluations and negotiations. Audits software usage to ensure compliance with associated licensing agreements.
- Supervises the Application Support Engineer, Network Specialist and End-User Support Analyst. Establishes performance goals, conducts performance appraisals and provides ongoing mentoring.
- Manages and coordinates various technology projects as required, ensuring company resources are utilized appropriately and within budget. Identifies and analyzes systems requirements and defines project scope and deliverables.
- Develops and promotes the adoption of internal I.T. governance policies based on the ITIL framework.
- Provides general, technology support to meet the day-to-day needs of Carnegie's end user community.

New Video Group, Inc. – New York, New Yorklocation **2000 – 2008**

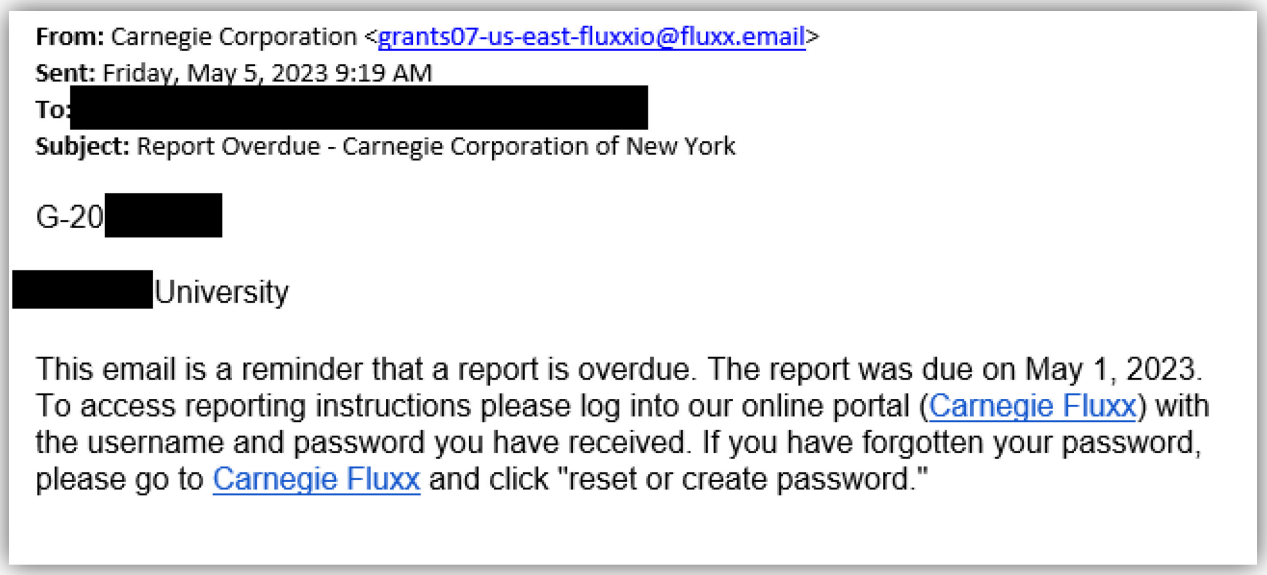
Director of IT *2006 - 2008*
IT Manager *2000 - 2006*

EDUCATION

The Cooper Union - Albert Nerkin School of Engineering **2000**

Bachelor of Science, Engineering

EXHIBIT 2



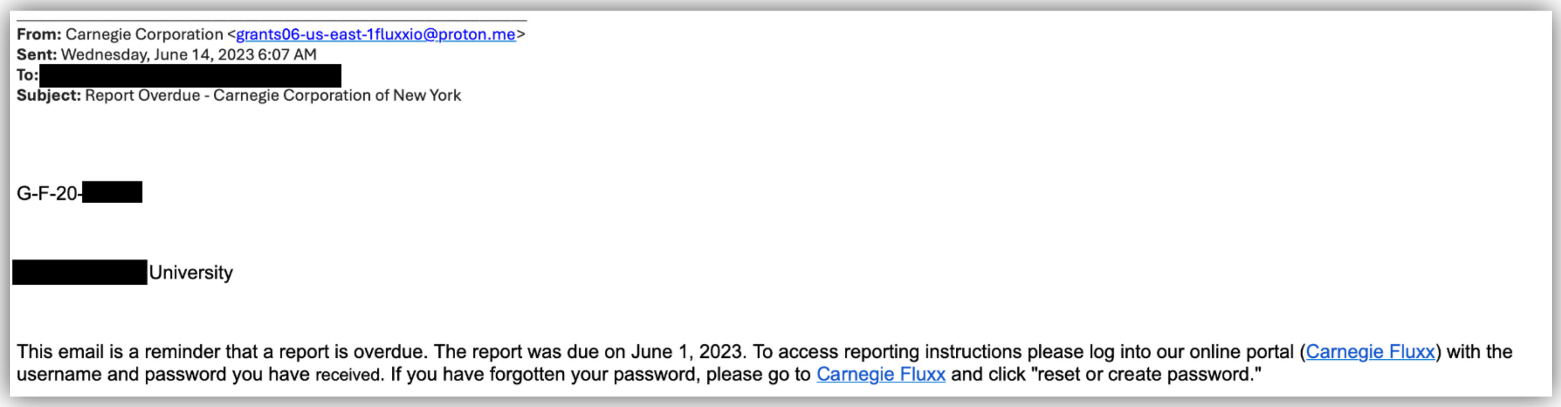
From: Carnegie Corporation <grants07-us-east-fluxxio@fluxx.email>
Sent: Friday, May 5, 2023 9:19 AM
To: [redacted]
Subject: Report Overdue - Carnegie Corporation of New York

G-20[redacted]

[redacted] University

This email is a reminder that a report is overdue. The report was due on May 1, 2023. To access reporting instructions please log into our online portal (Carnegie Fluxx) with the username and password you have received. If you have forgotten your password, please go to Carnegie Fluxx and click "reset or create password."

Image 1.



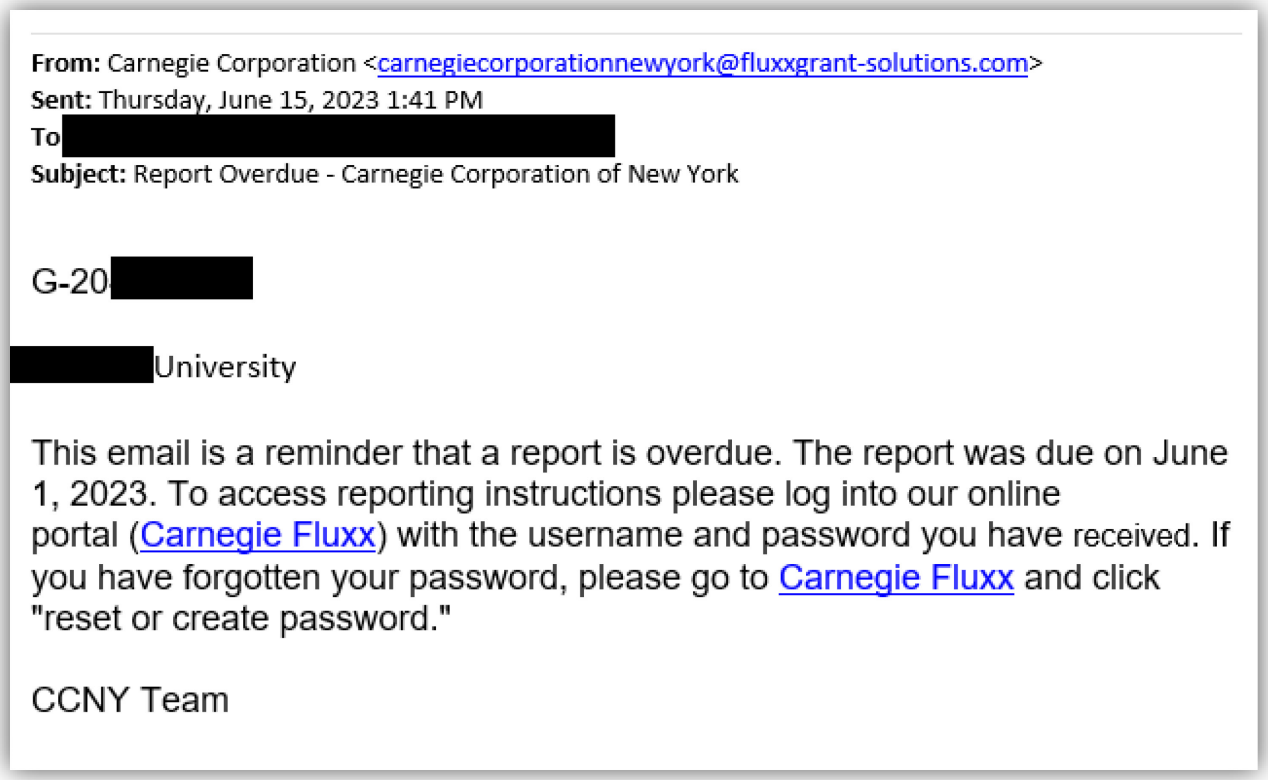
From: Carnegie Corporation <grants06-us-east-1fluxxio@proton.me>
Sent: Wednesday, June 14, 2023 6:07 AM
To: [redacted]
Subject: Report Overdue - Carnegie Corporation of New York

G-F-20-[redacted]

[redacted] University

This email is a reminder that a report is overdue. The report was due on June 1, 2023. To access reporting instructions please log into our online portal (Carnegie Fluxx) with the username and password you have received. If you have forgotten your password, please go to Carnegie Fluxx and click "reset or create password."

Image 2.



From: Carnegie Corporation <carnegiecorporationnewyork@fluxxgrant-solutions.com>
Sent: Thursday, June 15, 2023 1:41 PM
To [redacted]
Subject: Report Overdue - Carnegie Corporation of New York

G-20[redacted]

[redacted]University

This email is a reminder that a report is overdue. The report was due on June 1, 2023. To access reporting instructions please log into our online portal (Carnegie Fluxx) with the username and password you have received. If you have forgotten your password, please go to Carnegie Fluxx and click "reset or create password."

CCNY Team

Image 3.

From: Carnegie Corporation <grants06+2Dus+2Deast+2D1fluxxio=proton.me@bf01.eu1.hubspotfree.net>
August 7, 2023 1:44 AM
To: [redacted]
Subject: Report Overdue - Carnegie Corporation of New York

G-20-[redacted]

[redacted]

Dear [redacted]

This email is a reminder that a interim report is overdue. The report was due on August 1, 2023. To access reporting instructions please log into our online portal (Carnegie Fluxx) with the username and password you have received. If you have forgotten your password, please go to Carnegie Fluxx and click "reset or create password."

Image 4.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Microsoft Corporation, a Washington State Corporation, NGO-ISAC, a New York State Non-Profit Organization, Plaintiffs, v. John Does 1-2, Controlling A Computer Network and Thereby Injuring Plaintiff and Its Customers, Defendants.	Civil Action No. **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5.1**

DECLARATION OF NATALIA KRAPIVA IN SUPPORT OF APPLICATION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, Natalia Krapiva, declare as follows:

1. I am Senior Tech-Legal Counsel at Access Now, an international non-governmental non-profit organization working to defend and extend the digital rights of people and communities at risk, with particular focus on privacy and data protection, freedom of expression and assembly, digital security, and connectivity.[1] I make this declaration in support of Microsoft's and NGO-ISAC's Application for an Emergency Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction. I make this declaration of my own personal knowledge or on information and belief where indicated. If called as a witness, I could and would testify competently to the truth of the matters set forth herein.

[1] Available at https://www.accessnow.org/.

2. In my role at Access Now, I serve on the Legal team to shape Access Now's legal advocacy and accountability efforts, including through investigations and strategic litigation. I also work closely with Access Now's Digital Security Helpline,[2] which provides direct technical assistance to "civil society" which are the wide array of individuals, non-governmental and not-for-profit organizations, and community groups that participate in public life, advancing the interests and values of the communities they serve or represent, based on ethical, cultural, political, scientific, religious, philanthropic, or other considerations. For Access Now, members of civil society include journalists, activists, human rights defenders, and other public interest groups and individuals who share the common goals of justice, equality, and human dignity.[3] In that capacity, I often participate in the investigations of phishing, malware, and other digital attacks by closely working with the victims of such attacks and ensuring that the Helpline investigations are informed by sound legal strategy and guidance to maximize effective redress. For example, I have worked on Access Now's investigations of the use of the Pegasus spyware against civil society in Armenia,[4] Serbia,[5] as well as against Russian and Belarusian civil society living in exile in Europe.[6] In particular, I provided legal and risk guidance to the Helpline team, and coordinated with the victims, media, and all the relevant stakeholders on the publications of our findings.

3. At Access Now, I also work on drafting and submitting legal filings in the U.S. and international courts on issues related to spyware, internet shutdowns,[7] encryption,[8] among others. For example, I led the drafting and submission of an amicus brief in the Ninth Circuit Court of

[2] For more information on the Access Now Digital Security Helpline, see https://www.accessnow.org/help.
[3] U.N. Human Rights, Office of the High Commissioner, *Civil Society Resources for NGOs, human rights defenders, and other actors in civic space*, available at https://www.ohchr.org/en/resources/civil-society.
[4] Available at https://www.accessnow.org/publication/armenia-spyware-victims-pegasus-hacking-in-war/.
[5] Available at https://www.accessnow.org/spyware-attack-in-serbia/.
[6] Available at https://www.accessnow.org/publication/hacking-meduza-pegasus-spyware-used-to-target-putins-critic/; https://www.accessnow.org/publication/civil-society-in-exile-pegasus/.
[7] Available at https://www.accessnow.org/press-release/nigeria-twitter-ban-ecowas-court/.
[8] Available at https://www.accessnow.org/press-release/telegram-russia-ecthr-protect-encryption/.

Appeals case, *WhatsApp v. NSO Group*. Similar to this Star Blizzard litigation, the *WhatsApp* case involved members of civil society who were also targeted by threat actors. The amicus brief submitted by Access Now included testimonies from those victims, just as this declaration includes testimonies of members of civil society who were targeted by threat actors.[9] Prior to Access Now, I served as an Assistant District Attorney (ADA) at the Kings County District Attorney's Office in New York. My duties as an ADA included analyzing evidence, drafting legal submissions, making court appearances, and working with victims and witnesses to build cases for criminal prosecution. Prior to that, I held a variety of internships and full-time positions in the United States and internationally with the New York County District Attorney's Office, Queens County District Attorney's Office, New York State Attorney General's Office, the Human Rights Center at the University of California, Berkeley, School of Law, the Office of the United Nations (UN) High Commissioner for Human Rights, and the UN International Criminal Tribunal for the Former Yugoslavia, among others.

4. I obtained my Bachelor's Degree in Political Science from Columbia University in the City of New York and my Juris Doctor degree at the University of California, Berkeley, School of Law. A true and correct copy of the current version of my resume is attached to this declaration as **Exhibit 1**.

5. In my capacity as Senior Tech-Legal Counsel at Access Now, I worked closely with civil society victims in Access Now's investigation into STAR BLIZZARD. My declaration concerns STAR BLIZZARD's impact on civil society.

I. ACCESS NOW AND THE DIGITAL SECURITY HELPLINE

[9] Available at https://www.accessnow.org/press-release/nso-group-whatsapp-lawsuit-civil-society-amicus-brief/.

6. Access Now is an international non-governmental non-profit organization working to defend and extend the digital rights of people and communities at risk, with particular focus on privacy and data protection, freedom of expression and assembly, digital security, and connectivity.[10] Access Now began as an emergency response team of technologists working to help people get back online and ensure safe communications after the Iranian government blocked internet access and censored content during the 2009 Iranian election.[11] The organization now has a team of more than 100 people across 25 countries, including in the United States and Washington DC. Recognizing that in the 21st century, the threat of digital rights violations compound where they intersect with human rights abuses, Access Now works to hold governments and companies accountable for such violations and abuses in courts around the globe.[12]

7. The Access Now Digital Security Helpline (the Helpline) is a globally distributed team that provides 24/7 incident response and digital security advice to civil society around the world.[13] The Helpline offers real-time, free-of-charge, direct technical assistance and advice to civil society groups and activists, including independent media organizations, journalists, bloggers, activists, and human rights defenders. The Helpline's services are available in English, Arabic, French, German, Italian, Portuguese, Russian, Spanish, and Tagalog. These services include advising civil society individuals and organizations on such issues as threat modeling and risk assessment, secure communications, file storage, web browsing, and social media security, anonymity and censorship, as well as vulnerabilities, phishing, and malware, among others.[14]

[10] Available at https://www.accessnow.org/.
[11] Available at https://time.com/archive/6947035/iran-protests-twitter-the-medium-of-the-movement/.
[12] Available at https://www.accessnow.org/legal-team/.
[13] Available at https://www.accessnow.org/first-digital-security-helpline/.
[14] Available at https://www.accessnow.org/help/helpline-services/.

8. Since it began its work in 2013, the Helpline has responded to over 22,000 digital security requests from civil society in more than 160 countries. The Helpline is a member of CiviCERT, a network of Computer Emergency Response Teams (CERTs), Rapid Response teams, and independent Internet Content and Service Providers that help the civil society prevent and address digital security issues.[15] In 2019, the Helpline also became the first civil society helpdesk to join Forum of Incident Response and Security Teams (FIRST), a network of over 700 incident response and security teams across more than 110 countries, that use their combined knowledge, skills, and experience to promote a safer and more secure global electronic environment.[16]

9. The Helpline's Analyst team focuses specifically on analyzing evidence and investigating digital attacks against civil society, such as spyware, malware, spear phishing, and other attacks. Some of the recently published investigations featuring the Helpline's Analyst team's research includes investigation of NSO Group's sophisticated Pegasus spyware attacks against civil society in Jordan,[17] as well as Russian and Belarusian civil society based in Latvia, Poland, and Lithuania.[18]

II. ACCESS NOW'S INVESTIGATION INTO STAR BLIZZARD

10. In June 2024, Access Now's Helpline received a request from a well-known Russian independent media organization that faces persecution in Russia. At the time, many of the organization's staff were living in exile in countries throughout Europe and the Caucasus, while others remained in Russia. The media organization had received an email from an account that looked like it belonged to a staff member of a partner human rights organization headquartered in

[15] Available at https://www.civicert.org/.
[16] Available at https://www.accessnow.org/first-digital-security-helpline/.
[17] Available at https://www.accessnow.org/publication/between-a-hack-and-a-hard-place-how-pegasus-spyware-crushes-civic-space-in-jordan/.
[18] Available at https://www.accessnow.org/publication/civil-society-in-exile-pegasus/.

Washington DC. The email contained a PDF attachment which appeared to be “encrypted.” In order to “decrypt” the file, the receiver was presented with a “button” to click on that was in fact a URL link embedded within the PDF. One of the independent media’s staff members downloaded the file and tried to open it. Realizing that something was suspicious, the organization contacted the Helpline for assistance. The media organizations' Victim Impact Statement is attached as **Exhibit 2**.

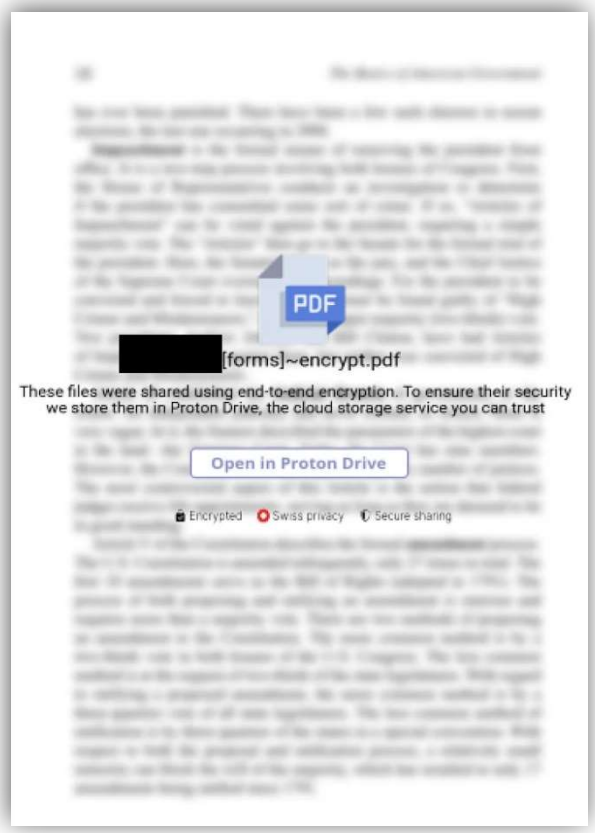


FIGURE 1.
Example of STAR BLIZZARD PDF lure. The phishing page is reached by clicking the link. The name of the file is redacted to remove the name of an impersonated organization for privacy and security reasons.

11. The Helpline’s Analyst Team analyzed the suspicious email and discovered that the email account was created on the day of the attack. The Analyst team also analyzed the code in

the URL link that was allegedly required to "decrypt" the PDF file. According to the Analyst team, the code in the link was designed to perform an automatic validation process that, once clicked, would determine certain information about the victim's computer, like the operating system and the system languages, before delivering specific web content. Depending on whether or not the recipient passed the check, they would be redirected either to a page designed to steal their credentials, or a benign page.

12. While the Helpline could not proceed to the next stage to conclusively determine whether or not this attack succeeded, it alerted its peer organization, the Citizen Lab[19] at the Munk School of Global Affairs and Public Policy, University of Toronto (the Citizen Lab) to help further analyze the incident. Subsequently, the Citizen Lab's research determined that the email received by the independent media organization was a highly targeted spear phishing attack (a digital attack that uses carefully tailored information that aligns with a target's personal and professional experiences and activities) by a Russia-based threat group known as STAR BLIZZARD[20] (also known as COLDRIVER,[21] SEABORGIUM, and CALLISTO,[22] among other names).[23] According to the United States and other governments, this group is a subordinate of the Russian Federal Security Service (FSB)'s Center 18.[24]

13. Between June and August 2024, Access Now analyzed five cases of STAR BLIZZARD phishing attacks, with several additional cases analyzed by the Citizen Lab. The

[19] The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs at the University of Toronto, Canada. It was founded by Ronald Deibert in 2001. The laboratory studies information controls that impact the openness and security of the Internet and that pose threats to human rights.
[20] Available at https://www.microsoft.com/en-us/security/blog/2023/12/07/star-blizzard-increases-sophistication-and-evasion-in-ongoing-attacks/.
[21] Available at https://blog.google/threat-analysis-group/google-tag-coldriver-russian-phishing-malware/.
[22] Available at https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-341a.
[23] Available at https://citizenlab.ca/2024/08/sophisticated-phishing-targets-russias-perceived-enemies-around-the-globe/.
[24] Available at https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-341a.

details of these investigations are outlined in our respective publications. Access Now's main publication on the investigation is attached to this declaration as **Exhibit 3**.[25] Access Now Helpline's Technical brief is attached to this declaration as **Exhibit 4**.[26] The Citizen Lab's publication outlining their respective investigation is attached to this declaration as **Exhibit 5.**[27]

14. Among the targets identified in the Access Now and Citizen Lab's STAR BLIZZARD investigation are prominent Russian and Belarusian human rights organizations, independent media organizations, as well as former U.S. Ambassador to Ukraine, Steven Pifer. In addition, the hackers behind STAR BLIZZARD also impersonated several DC-based human rights non-governmental organizations (NGOs), as well as another former U.S. Ambassador, to send phishing emails.

15. Since finalizing our publication, Access Now has been investigating several additional phishing cases. Access Now and the Citizen Lab believe that at least one of these additional cases is associated with the STAR BLIZZARD campaign.

16. Access Now also believes that STAR BLIZZARD has likely impacted many more civil society actors from Russia, Belarus, Ukraine, the United States, Western Europe, and beyond. Many organizations and individuals in the civil society space working for human rights in Russia and the region have shared with us that they also received phishing emails that are similar to STAR BLIZZARD or know someone in the community who received such emails. A leading Ukrainian digital security organization and a CiviCERT member, Digital Security Lab (DSL) Ukraine, has shared with us that they have been documenting "waves of targeted phishing attacks using

[25] Also available at https://www.accessnow.org/russian-phishing-campaigns/.
[26] Also available at https://www.accessnow.org/wp-content/uploads/2024/08/Spearphishing-cases-in-Eastern-Europe-2022-2024-technical-brief.pdf.
[27] Also available at https://citizenlab.ca/2024/08/sophisticated-phishing-targets-russias-perceived-enemies-around-the-globe/.

malicious attachments" against Ukrainian civil society (see the Statement of DSL Ukraine attached as **Exhibit 6).** However, they are not always able to investigate these attacks further due to the lack of resources or inability to gather indicators (see the Statement of DSL Ukraine attached as **Exhibit 6).**

III. THE IMPACT OF STAR BLIZZARD ON SPECIFIC CIVIL SOCIETY ORGANIZATIONS AND INDIVIDUALS

17. STAR BLIZZARD's phishing campaign has inflicted substantial harm on specific individuals and organizations in the United States and internationally.

18. While some targets told us that they did not engage with the phishing emails, others were deceived into clicking on the phishing file or link and entering their user credentials. Even though Access Now did not directly observe credentials being passed back to the attacker's infrastructure, based on the targets' descriptions, it is likely that the attackers leveraged a tool that is specifically designed to capture the entered user credentials and enable unauthorized access. Microsoft documented such techniques used by STAR BLIZZARD in the past.[28]

19. At least one victim reported that after the attack, she lost access to her organization's Google account and one of her contacts received a similar phishing email impersonating her (see Victim Impact Statement attached as **Exhibit 7**). Some victims have also reported highly sensitive records contained in their email accounts leaked on the internet (see Victim Impact Statement attached as **Exhibit 8**). This makes it likely that the STAR BLIZZARD attackers were able to successfully obtain unauthorized access to at least some of the victims' online accounts.

[28] Available at https://www.microsoft.com/en-us/security/blog/2023/12/07/star-blizzard-increases-sophistication-and-evasion-in-ongoing-attacks/.

20. Most of the targets of STAR BLIZZARD attacks that Access Now and Citizen Lab investigated are Russian NGOs and independent media which defend human rights and democracy, aid refugees, political prisoners, or LGBTQ+ individuals, and report on state corruption, human rights violations, and Russia's illegal war in Ukraine. These organizations have staff located in Russia as well as living in exile around the world, including the United States and Washington DC. One of the targeted organizations in this investigation also works on human rights in Belarus, "Europe's last dictatorship"[29] and Russia's close ally.[30] For these civil society actors, the STAR BLIZZARD attacks are extremely dangerous, since their email accounts contain sensitive information about their staff's identities, activities, relationships, finances, and whereabouts which would likely be of interest to the Russian and Belarusian governments and affiliated actors (see Victim Impact Statements attached as **Exhibits 2, 8, and 9)**.

21. In both Russia and Belarus, these non-governmental organizations and independent media face severe persecution. Some have already experienced criminal prosecution, imprisonment, harassment, intimidation, blocking of their websites, revocation of their legal status, and even physical attacks. Some have been prosecuted under the Russian "fake news" law, which punishes sharing any information about Russia's invasion of Ukraine that contradicts Russian government's position with up to 15 years of imprisonment.[31] Most have received legal designations as "undesirable organizations" and "foreign agents" under the two Russian laws that penalize any cooperation between Russian civil society and Western NGOs and officials and

[29] Available at https://www.economist.com/the-economist-explains/2021/05/25/why-belarus-is-called-europes-last-dictatorship.
[30] Available at https://www.cfr.org/backgrounder/belarus-russia-alliance-axis-autocracy-eastern-europe.
[31] Available at https://www.reuters.com/world/europe/russia-introduce-jail-terms-spreading-fake-information-about-army-2022-03-04/.

which, according to human rights groups,[32] US government,[33] European Union,[34] Organization for Security and Co-operation in Europe (OSCE),[35] and UN experts[36] are repressive tools of retaliation against dissenters. These are repercussions for activities that would be protected under the US First Amendment, such as defending the human right to peaceful protest, supporting political prisoners, or criticizing the war in Ukraine.

22. Due to these threats, the affected organizations and individuals often take multi-layered steps to secure their identities, contact information, and locations, to protect themselves, as well as their staff, partners, clients, and journalistic sources, many of whom are still located in Russia or Belarus. The STAR BLIZZARD phishing campaign was designed to compromise these security measures.

23. One of the targeted individuals in the STAR BLIZZARD attack is Polina Machold, Publisher of Russian independent investigative outlet, Proekt Media. Polina received a STAR BLIZZARD phishing email from an account impersonating a fellow journalist from a U.S. government-funded international media organization (see Victim Impact Statement attached as **Exhibit 9**). Proekt is famous for its high-profile investigations into Russian state corruption, repression, and war crimes in Ukraine, especially involving Russian President Vladimir Putin and his inner circle.[37] These types of investigations require working with sensitive sources and journalists on the ground in Russia who may be in grave danger if their involvement is exposed. Proekt is already a "foreign agent" media that is banned in Russia, with its journalists forced into exile in Europe, United States, and Central Asia (see Victim Impact Statement attached as **Exhibit**

[32] Available at https://www.hrw.org/news/2023/07/25/russia-bill-bans-work-most-foreign-groups.
[33] Available at https://www.state.gov/reports/2023-country-reports-on-human-rights-practices/russia/.
[34] Available at https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)729297.
[35] Available at https://www.osce.org/files/f/documents/7/5/526720.pdf.
[36] Available at https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=25007.
[37] Available at https://www.proekt.media/en/home/.

9). Proekt was also the first news outlet designated as "undesirable" by the Russian government.[38] Such designation imposes administrative and criminal sanctions on those who collaborates with the organization or even shares their articles on social media.[39] The media's founder, Roman Badanin is known as a personal enemy of Vladimir Putin.[40] According to Polina, Proekt was already "dealing with hacking attempts from Russian State-linked groups," but STAR BLIZZARD "was the most elaborate attempt" to digitally compromise the organization (see Victim Impact Statement attached as **Exhibit 9**).

24. Another independent media organization has also shared with us that the STAR BLIZZARD attack was "the most significant and malicious challenge [they had] ever faced" (see Victim Impact Statement attached as **Exhibit 2**). The attack prompted the media, which was also declared "undesirable" by the Russian government and had four of its staff arrested in the past, to sever working relationships with their staff in Russia and attempt to evacuate some of them (see Victim Impact Statement attached as **Exhibit 2**). According to the organization, they "now live with the distressing knowledge that their [staff's] homes may be raided, and they could face arrest for collaborating with an organization that the Russian government has unjustly labeled as 'undesirable.'" (see Victim Impact Statement attached as **Exhibit 2**).

25. Another STAR BLIZZARD target is a Russian human rights lawyer and the head of a major civil society organization that assists individuals fleeing Russia due to political persecution and their anti-war position (see Victim Impact Statement attached as **Exhibit 10**). For its important work, the Russian government has recently labeled the organization as a "foreign agent." According to the lawyer, while she did not open the STAR BLIZZARD phishing PDF, if

[38] Available at https://rsf.org/en/proekt-first-russian-media-outlet-be-declared-undesirable.
[39] Available at https://ipi.media/russia-must-stop-designating-media-as-undesirable/.
[40] Available at https://www.washingtonpost.com/opinions/2021/09/01/roman-badanin-russia-foreign-agent-law-journalists/.

the attempts to compromise her "had been successful, the potential for harm would have been catastrophic" (see Victim Impact Statement attached as **Exhibit 10**). Such a breach would expose sensitive information about the organization's clients, including their location and the details of their asylum cases, compromising the attorney-client confidentiality and potentially resulting in arrest, imprisonment, "or worse" for these individuals and their families (see Victim Impact Statement attached as **Exhibit 10**). This is especially concerning given that the Russian security services, and FSB in particular, have been reportedly actively engaged in assassinations of asylum seekers and regime critics around the world.[41]

26. For those Russian organizations and individuals who have not been labeled yet as "foreign agents" or "undesirable," there is also an additional risk that Russia can use any contact between them and US and Western-based organizations revealed through their email communications as a pretext for such designations. This could lead to such individuals being criminally charged[42] and imprisoned.[43] For example, another STAR BLIZZARD victim that works with a Russian independent media organization has shared that Russian propaganda channels are urging authorities to imprison their staff and declare the outlet "undesirable" (see Victim Impact Statement attached as **Exhibit 8**). The media organizations' email communications with funders could provide the Russian authorities with the needed pretext for such persecution (see Victim Impact Statement attached as **Exhibit 8**). "Undesirable" designation would especially affect the media's journalists and editors based in Russia, as well as the Russian people across the country who share their opinions and life stories with the media (see Victim Impact Statement attached as

[41] Available at https://www.ft.com/content/46753c29-78f9-485f-8f02-8b203557c40e; https://www.bellingcat.com/news/uk-and-europe/2020/02/17/v-like-vympel-fsbs-secretive-department-v-behind-assassination-of-zelimkhan-khangoshvili/.
[42] Available at https://www.hrw.org/news/2017/06/05/russia-rights-activist-facing-charges.
[43] Available at https://www.amnesty.org/en/latest/news/2022/05/russia-activist-mikhail-iosilevich-jailed-for-collaborating-with-so-called-undesirable-organization/.

Exhibit 8). Thus, the unlawful hacking at issue here obstructs the free flow of information and ideas and enables potential follow-on abuses and further violations of fundamental rights. As one media organization put it, "having [their] most sensitive data fall into the hands of [their] worst enemy has left [them] vulnerable and exposed to further oppression" (see Victim Impact Statement attached as **Exhibit 2**).

27. This is why most of the individuals and organizations that Access Now and the Citizen Lab have worked with in the course of the STAR BLIZZARD phishing campaign investigation, requested to stay anonymous and not be mentioned in our public reports. Some individuals were so fearful and emotionally distressed by their information being further exposed to the FSB that they were reluctant to come forward and share any information about the attack even anonymously. Some also experienced shame that they were tricked into interacting with malicious emails and attachments, which may have put their colleagues, clients, and partners at risk.

28. Some STAR BLIZZARD phishing victims have shared with us that they are concerned about the psychological stress caused to their colleagues and clients by the mere realization that the organization was targeted by an FSB-affiliated actor, even if the attack was not successful. The human rights lawyer who was targeted by STAR BLIZZARD shared that her organization works with individuals "who are already under immense pressure due to political threats" they are facing (see Victim Impact Statement attached as **Exhibit 10**). Every new phishing attempt heightens fears that her organization's "efforts to protect human rights and support those fleeing persecution could be undermined" (see Victim Impact Statement attached as **Exhibit 10**).

29. Victims were also concerned that if their community and colleagues learn that they were targeted or impersonated by the STAR BLIZZARD hackers, their reputation and the

reputation of their organization would be severely damaged and people may stop trusting their communications in the future. One of the victims shared with us that a successful STAR BLIZZARD compromise would also "erode the trust" the clients place in her organization, damaging their ability to provide crucial support (see Victim Impact Statement attached as **Exhibit 10**).

30. Indeed, STAR BLIZZARD operations are designed to erode the trust and relationships between civil society organizations and their supporters. In several cases investigated by Access Now and the Citizen Lab, the STAR BLIZZARD emails which targeted Russian and Belarusian civil society organizations impersonated prominent U.S. and especially DC-based organizations. Some of the phishing emails contained the names of these organizations in the malicious PDF files purporting to be human rights reports or other important documents (see **FIGURE 1)**. Such tactics may cause the victims to be reluctant to open emails and attachments from their partner organizations in the future, producing a chilling effect[44] on speech and shrinking civic space.

31. In some cases, the hackers behind STAR BLIZZARD, by using the information they likely obtained from compromising the victim's emails, turned to impersonating the victim to hack their colleagues, partners, and associates. We believe this is what happened to the head of a UK-based organization that helps Russian dissidents and LGBTQ+ individuals, organizes in support of democracy, and raises funds for Ukraine. She received a STAR BLIZZARD phishing email impersonating a prominent DC-based Russian human rights defender and the founder of a US human rights organization that promotes democracy in Russia (see Victim Impact Statement attached as **Exhibit 7**). After the attack, the name of the victim was used in a phishing attack

[44] Available at https://www.opensocietyfoundations.org/publications/the-concept-of-chilling-effect.

against another prominent individual working with civil society, "eroding trust in an already fragile environment" (see Victim Impact Statement attached as **Exhibit 7**).

32. Amongst those affected by the STAR BLIZZARD operations are also former US Ambassadors. For example, as the Citizen Lab revealed, former U.S. Ambassador to Ukraine, Steven Pifer, currently working with the Center for International Security and Cooperation (CISAC) at Stanford University,[45] as well as DC-based Brookings Institution,[46] was targeted with a STAR BLIZZARD phishing email impersonating another fellow Ambassador (see the Citizen Lab's report attached as **Exhibit 5**). The Citizen Lab stated in their report that they believe that Ambassador Pifer may have been targeted for his extensive networks among sensitive civil society communities, including high-risk individuals from Russia (see the Citizen Lab's report attached as **Exhibit 5**). Such sophisticated attacks that use social engineering – where a malicious actor poses as someone the victim knows and trusts in order to deceive them and obtain unauthorized access to their computer systems[47] – undermine professional and personal relationships and damage confidence and trust between people.

33. Finally, in addition to putting individuals' and organizations' safety, relationships, and reputation at risk, the STAR BLIZZARD attacks have also significantly disrupted the ability of the civil society affected by the phishing campaign to do their important human rights work. One victim shared that because her Gmail account was locked for three days after the phishing attack, her organization was "severely hindered in [its] ability to assist another NGO with their grant application for the evacuation of LGBTQA+ individuals persecuted in Russia" (see Victim Impact Statement attached as **Exhibit 7**). The organization also lost access to their calendar and

[45] Available at https://cisac.fsi.stanford.edu/.
[46] Available at https://www.brookings.edu/.
[47] Available at https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks

missed other critical communications, significantly setting back their operations (see Victim Impact Statement attached as **Exhibit 7**). In the aftermath of the phishing attack, the affected organization also had to undertake a comprehensive review of their digital and personal security, which took over two weeks and required costly resources from an organization that has no paid staff, adding "an enormous workload [and] straining the mental and physical health of [their] activists, who are already working tirelessly" (see Victim Impact Statement attached as **Exhibit 7**).

34. Another organization shared that following the attack, "[t]he financial and administrative burden of evacuating [their] team members who agreed to leave Russia [had] been immense" (see Victim Impact Statement attached as **Exhibit 2**). The STAR BLIZZARD operation has left the organization's entire team "distressed and unable to work effectively for an extended period following the attack" (see Victim Impact Statement attached as **Exhibit 2**).

IV. THE IMPACT OF STAR BLIZZARD ON CIVIL SOCIETY AS A WHOLE

35. Beyond the specific individuals and organizations targeted or impersonated in this phishing campaign, the STAR BLIZZARD has a profound effect on civil society, the civic space, and the security of journalists and human rights defenders as a whole.

36. The hackers behind the STAR BLIZZARD campaign use sophisticated techniques that carefully study the individuals and organizations, their work, their contacts and relationships, and other surrounding context, and exploit it to steal credentials and conduct espionage on behalf of the Russian regime. These tactics instill fear and reluctance in the civil society to communicate and participate in civic spaces.

37. All individuals, and especially journalists and activists who often live in exile or are operating in extremely repressive environments, rely on the internet and online

communications for exercising their fundamental rights, the same rights protected by the U.S. Constitution and affirmed in international law. Weaponizing online email platforms to steal credentials and conduct espionage violates not only the fundamental right to privacy, but also rights to receive and impart information, organize, and peacefully assemble for civic and political action, online and off. Hacking and surveillance of journalists and independent media also violates press freedom, explicitly protected under the U.S. First Amendment.

38. STAR BLIZZARD also undermines the trust in digital security among civil society. In their recommendations, digital security organizations often advise not to interact with strangers and avoid "suspicious" emails, links, or attachments. However, the malicious emails and attachments in the STAR BLIZZARD phishing campaign were not immediately "suspicious," but, on the contrary, looked like they were coming from a trusted source. Since STAR BLIZZARD hackers are so effective at impersonating the individuals and organizations known to the victim, it could be very difficult to immediately realize you are communicating with a malicious actor.

39. In some ways, sewing confusion and self-doubt is the goal. Thus, the STAR BLIZZARD attacks instill in the victims and others in the community a sense that no matter how closely they follow digital security recommendations, it will not be enough to make them feel secure. This leaves them feeling like in order to achieve security, they would need to stop communicating altogether or otherwise not bother following digital security protocols. This deters civil society actors from communicating and associating online, resulting in a chilling effect, and also discourages them from taking digital security measures.

V. COURT MUST TAKE ACTION TO ADDRESS THE HARMS OF STAR BLIZZARD

40. Since we published our investigation, more civil society individuals are contacting Access Now with suspected phishing cases. We believe that at least some of them were targeted by STAR BLIZZARD. This leads us to think that the attacker is still active and not deterred despite governments, companies, and civil society exposing their malicious activities.

41. Thus, we are asking the court to take urgent action to prohibit the threat actors behind STAR BLIZZARD from continuing to engage in the harmful and illegal behavior that targets civil society organizations and their partners in the United States and internationally. Stepping in and preventing STAR BLIZZARD from relying on U.S. internet infrastructure, such as domain registries/registrars and IP address hosting providers, will help protect vulnerable civil society and independent media organizations from being victimized, and the respectable U.S. NGOs and individuals, like Ambassador Pifer, from having their good name and reputation exploited for espionage and other harmful activities.

42. In addition, by allowing the discovery in this case and subpoenaing the domain registrars or hosting providers used by STAR BLIZZARD, the court has an opportunity to reveal the information about the attackers that could enable further enforcement actions, including potential public notices, criminal charges, and sanctions, which could help ensure accountability and some redress for the victims.

43. These actions would be consistent with U.S. domestic law, as well as the United States' international human rights obligations, such as the International Covenant on Civil and Political Rights (ICCPR),[48] which the United States ratified in 1992,[49] and which guarantees the

[48] Available at https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.
[49] Available at https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&clang=_en.

protection of the right to privacy and the freedoms of expression, peaceful assembly and association, and political participation.

44. This will also be in line with the United States' domestic policies, such as calling out governments for "abusing technological advancements to infringe on the democratic process and on the human rights of their constituents"[50] and protecting civil society from cyber threats,[51] as well as its international commitments, priorities, and engagements related to defending free and secure internet. For example, as a founding member of the Freedom Online Coalition (FOC), which is a coalition of 40 governments that work together and engage with civil society and the private sector to support internet freedom, the United States has led on a number of statements aimed at protecting civil society from threats like STAR BLIZZARD.[52] In October 2023, during the 54th session of the UN Human Rights Council, acting as chair of the FOC, the United States presented a Joint Statement on the Heightened Risks Associated with Surveillance Technologies and the Importance of Safeguards in the Use of These Tools.[53] The statement builds on the FOC's March 2023 Guiding Principles on Government Use of Surveillance Technologies,[54] and calls on governments to take steps to ensure the use of these technologies is lawful and responsible, in accordance with states' domestic law and international obligations and commitments.[55] Similarly, in its 2020 Joint Statement on the Human Rights Impact of Cybersecurity Law, Practices and Policies, the FOC recommended that states "develop and implement cybersecurity-related laws, policies and practices in a manner consistent with international human rights law, and seek to

[50] Available at https://www.state.gov/commemorating-the-international-day-of-democracy-3/.
[51] Available at https://www.cisa.gov/news-events/alerts/2024/05/14/cisa-and-partners-release-guidance-civil-society-organizations-mitigating-cyber-threats-limited.
[52] Available at https://freedomonlinecoalition.com/.
[53] Available at https://freedomonlinecoalition.com/joint-statement-heightened-risks-associated-with-surveillance-technologies-and-the-importance-of-safeguards-in-the-use-of-these-tools/.
[54] Available at https://freedomonlinecoalition.com/guiding-principles-on-government-use-of-surveillance-technologies/.
[55] Available at https://freedomonlinecoalition.com/joint-statements/.

minimize potential negative impacts on vulnerable groups and civil society, including human rights defenders and journalists."[56] Previous FOC work, endorsed by the U.S. government, emphasized that such national law and policies should consider "the disproportionate threats faced by individuals and groups at risk" and "protect and promote human rights.[57] Other U.S.-led initiatives, like the Summit for Democracy, put human rights and democracy at the heart of the U.S. foreign policy.[58]

45. An effective enforcement action by this court would send a strong signal to the adversaries and allies alike that the United States will not tolerate threat actors like STAR BLIZZARD using U.S.-based infrastructure to target human rights defenders and journalists and destroy human rights, democracy, and the civic space. The court must help protect the rights and liberties of the civil society individuals that risk their lives daily to protect the values that the United States champions at home and abroad.

46. Finally, an enforcement action would also reward the courageous civil society victims for coming forward, allowing organizations like Access Now and the Citizen Lab to investigate the STAR BLIZZARD attacks against them, and sharing their stories and the impact that the attacks has had on them. Seeing a direct and concrete action from the US courts will also encourage other victims to speak out.

47. In the words of one of the STAR BLIZZARD's civil society victims, we "implore the court to consider the gravity of this attack [and] the lasting harm[s] it has caused" and to urgently address these harms.

---

[56] Available at https://freedomonlinecoalition.com/wp-content/uploads/2021/06/FOC-Joint-Statement-on-the-Human-Rights-Impact-of-Cybersecurity-Laws-Practices-and-Policies.pdf.

[57] Available at https://freeandsecure.online/recommendations/.

[58] Available at https://www.state.gov/further-information-the-summit-for-democracy/.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed this 23rd day of September, 2024, in Nuremberg, Germany.

_____

Natalia Krapiva

Senior Tech - Legal Counsel
Access Now

Natalia Krapiva J.D.

Berlin, Germany ✉ natalia@accessnow.org LinkedIn

SUMMARY

- ✔ Highly confident and skilled legal practitioner bringing 8+ years of increasingly responsible legal experience with US and international organizations and a passion for litigation, international human rights, and technology policy issues.
- ✔ Expert understanding of human rights law and practice, the international political system, and the internet. Proven ability to identify emerging issues and use legal mechanisms to prevent and mitigate threats.
- ✔ Recognized by senior management as a strategic and creative thinker who can provide expert and tactical advice to the organization, the team, and management.
- ✔ Demonstrable ability to manage competing and urgent tasks, as well as long-term and sustained projects, taking them all to completion while regularly reporting on progress to relevant stakeholders.
- ✔ Extensive portfolio of successful legal briefs, written publications, and press interviews.
- ✔ Juris Doctor (UC Berkeley), licensed in New York (USA), bilingual fluency in English/Russian and basic German.

PROFILE

❖ **Results Oriented:** Led successful business and human rights advocacy campaigns including against Sandvine (the company withdrew from Belarus and was added to the Entity List by the US Treasury Department) and Cellebrite (the company had to provide information to the US SEC on human rights risks of its technologies).

❖ **Ability to Analytically Solve Issues:** Analyzed court decisions and drafted multiple motions, expert opinions, and amicus brief, including the successfully filed amicus brief in the WhatsApp v. NSO 9th Circuit case, highlighting for the court the human rights implications of commercial spyware and its impact on victims.

❖ **Litigation and Investigation Experience**: Worked on over 300 cases as an Assistant District Attorney, ranging from minor assaults and DUIs to human trafficking and felony assaults, including working with victims and witnesses, preparing subpoenas, and appearing in court. As a Senior Tech-Legal Counsel, drafted and submitted over 20 legal filings on issues related to spyware, internet shutdowns, business and human rights, among others. Led and provided legal assistance to investigations of state-sponsored spyware attacks in El Salvador, Armenia, Serbia, EU, and beyond, including working with victims, media, and all the relevant stakeholders.

EMPLOYMENT EXPERIENCE

Access Now, Berlin, Germany **May 2019 – Present**

Defends and extends the digital rights of people and communities at risk

Senior Tech-Legal Counsel

- Work with the Digital Security Helpline to prevent and mitigate legal obstacles to its work, to its beneficiaries' work, and to the greater digital security ecosystem.
- Serve on the Legal team to shape Access Now's strategic direction and other accountability efforts, including thorough forensic investigations and strategic and impact litigation by Access Now and its partner organizations.

- Develop, support and represent Access Now in global partnerships and coalitions, such as global network of impact litigants, and identifying opportunities to promote new jurisprudence to better protect users at risk and advance digital rights under law.
- Serving as advisor to the General Counsel on external issues, including legal risks.
- Contributing to information gathering and norm development activities by Access Now's Policy and Advocacy team, including through input into blog posts, legal briefs, reports, and other written documents, ensuring they are appropriately informed by risks and threats to Access Now's mission.

Kings County District Attorney's Office, Brooklyn, NY **October 2018 – May 2019**

Assistant District Attorney

- Analyzed assigned cases, prepared cases for trial, and appeared in criminal court.
- Interviewed witnesses, victims, and police officers to collect evidence and to make critical decisions to support court proceedings.

UC Berkeley School of Law Human Rights Center, Berkeley, CA September 2016 - May 2018

Promotes human rights and international justice worldwide

Human Rights Investigations Lab Intern/Mentor/Legal Advisory Board Member

- Conducted cutting-edge open-source investigations into human rights and criminal law violations.
- Provided mentorship and guidance to students and management on legal and ethical matters and helped inform investigative strategies and future Lab projects.

Independent Research **July 2017 - May 2019**

Research Assistant

- Assisted the former Benetech Vice President for Human Rights in advising on the digital needs of the newly-established United Nations International, Impartial and Independent Mechanism on Syria, by researching innovative ways of conducting investigations.

Queens County District Attorney's Office, New York, NY **May 2017 - July 2017**

Legal Intern, Homicide Trials Bureau

- Assisted Homicide Trials Assistant District Attorneys in all stages of trials by conducting legal and factual research and drafting court motions.

Office of the UN High Commissioner for Human Rights, Geneva, CH **Jan 2017 - April 2017**

Intern, Legal Policy Office

- Assisted senior staff in drafting, reviewing, and editing legal documents, including amicus briefs and human rights reports.
- Researched and wrote comprehensive memos on complex and/or novel issues of International Humanitarian Law (IHL), International Human Rights Law (IHRL) and International Criminal Law, including the relationship between IHL and IHRL, rights of children in armed conflict, and non-state armed groups.

UC Berkeley International Human Rights Law Clinic, Berkeley, CA **Sept 2016 - Dec 2016**

Clinical Intern

- Conducted fact and international legal research contributing to the drafting of a report on the issue of Sexual Exploitation and Abuse (SEA) in United Nations Peacekeeping Missions used to advocate for SEA victim redress.

Natalia Krapiva J.D.

International Criminal Tribunal for the Former Yugoslavia, The Hague **May 2016 - Aug 2016**

Legal Intern, Office of the Prosecutor, Trial Division

- Conducted legal and factual research, analyzed evidence and assisted trial attorneys with drafting and revising the Final Trial Brief and court motions for the Prosecutor v. Mladić case.

Manhattan District Attorney's Office, New York, NY **January 2014 - July 2015**

Legislative Analyst, Division of Legislative Affairs

- Conducted extensive research on the Apple/Google encryption and other legislative issues, convened NYS law enforcement stakeholders, and wrote comprehensive briefings for the DA.

Mobilization for Justice (MFY Legal Services), New York, NY **February 2013 - January 2015**

Disaster Response Legal Services Assistant

- Worked closely with Disaster Response Law Project attorneys on a range of tasks, which helped victims of Hurricane Sandy, including conducting client intakes, reviewing and organizing documents and databases, filing FEMA and insurance appeals, and filing complaints against contractors with relevant governmental agencies.

New York State Attorney General's Office, New York, NY **January 2012 - June 2012**

Intern

- Assisted the Bureau Chief with various projects and initiatives related to combating human trafficking including staff training, outreach, advocacy, and funding.

United States Senator Kirsten E. Gillibrand's Office, New York, NY January 2012 - March 2012

Casework Intern

- Assisted constituents with Social Security, Medicare, Medicaid, Education, SNAP, HEAP, and FEMA issues.

NYS DOL Division of Compliance & Education, New York, NY **June 2011 - August 2011**

Summer Intern

- Conducted legal research and research on immigrant community organizations and coalitions across the state to help the former Division of Immigrant Policies & Affairs to better serve immigrants.

OTHER RELEVANT EMPLOYMENT, INTERNSHIPS, & VOLUNTEER EXPERIENCE

East Bay Community Law Center, Berkeley, CA **April 2016**
Jewish Family & Vocational Service, Milltown, NJ **February 2013 – March 2013**
Columbia University, New York, NY **June 2010 – May 2011**
NJ Department of Labor, New Brunswick, NJ **July 2008 – July 2009**
Middlesex County College, Edison, NJ **September 2006 - April 2008**

EDUCATION

The University of California, Berkeley, School of Law, J.D. **2018**
International Law Certificate
Concentration: International Law
Human Rights and Technology Project: Conducted detailed research of cases where the International Criminal Court used open-source evidence, including Facebook and YouTube content, contributing to the Yale Law Journal publication by the Project supervisor.

Natalia Krapiva J.D.

Law Review: Wrote a research paper, published in the California Law Review, providing recommendations to the newly established International, Impartial, and Independent Mechanism on Syria to better utilize open source and clandestine documentary evidence.
Student Leader: International Human Rights Workshop, Central African Republic Project
Recipient: Herma Hill Kay Fellowship Award for Advancing Interests of Women in the Law and Elizabeth & Charles Tigar Public Interest Scholarship

Columbia University, New York, NY **2012**
B.A. in Political Science, Dean's List, Summa Cum Laude 3.9 GPA
Concentrations: International Relations, American Politics
Recipient: Arthur Ross Foundation Award in Political Science
Member: Phi Beta Kappa, GS Honor Society

Middlesex County College, Edison, NJ **2008**
A.A. in Communication, A.A. in Education, Dean's List, Summa Cum Laude 3.9 GPA

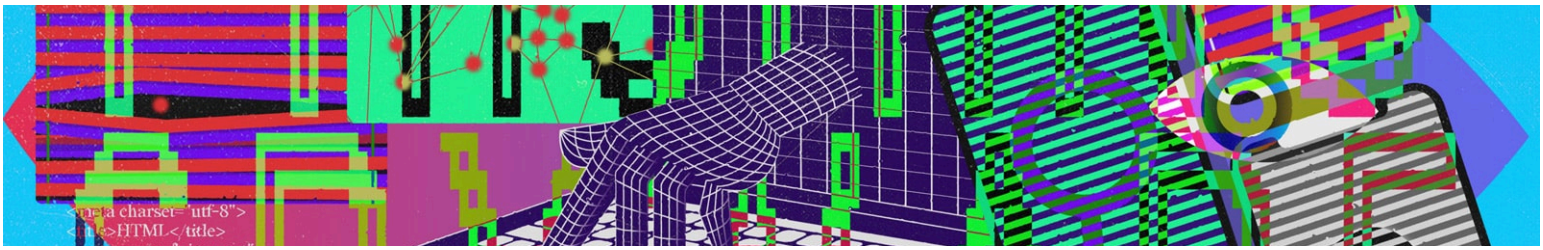
In June, we fell victim to a malicious attack perpetrated by the STARBLIZZARD/COLDRIVER hacker group, which is known to have ties to the Russian government and the Federal Security Service (FSB). As an entity whose primary adversary is the Russian government, having our most sensitive data fall into the hands of our worst enemy has left us vulnerable and exposed to further oppression.

The consequences of this attack have been far-reaching and severe. We were forced to immediately sever all work relationships with our highly skilled and dedicated team members based in Russia. While we offered assistance to help them flee the country, not everyone had the means or ability to do so. We now live with the distressing knowledge that their homes may be raided, and they could face arrest for collaborating with an organization that the Russian government has unjustly labeled as "undesirable."

This incident has been the most traumatic and damaging event our organization has ever faced. We have already experienced the consequences of such actions in the past, with a raid on our organization and four of our team members being placed under house arrest in 2021-2022. The financial and administrative burden of evacuating our team members who agreed to leave Russia has been immense, and our entire team has been left distressed and unable to work effectively for an extended period following the attack.

Even those of us who are in exile face heightened threats, particularly in countries like Georgia and Armenia, where many of our staff members are based. These countries are flooded with Russian undercover police who regularly kidnap people, making it an incredibly dangerous environment for our team. Furthermore, all of us in exile are unable to return to Russia, even if we worked anonymously until now, as the risk of imprisonment is too great, and no one can afford to take it until the current regime falls.

The actions of the STARBLIZZARD/COLDRIVER hacker group have dealt a devastating blow to our organization, one from which we are still reeling. This attack is the most significant and malicious challenge we have ever faced, and its impact will undoubtedly be felt for years to come. We implore the court to consider the gravity of this attack, the lasting harm it has caused to our organization and its members, and the ongoing threats we face as you deliberate on the appropriate course of action.



Caught on the net: Russia-linked phishing campaigns ensnare Russian and Belarusian civil society, as well as international NGOs

PUBLISHED: 14 AUGUST 2024
LAST UPDATED: 15 AUGUST 2024

Access Now's Digital Security Helpline and the Citizen Lab at the Munk School of Global Affairs & Public Policy at the University of Toronto ("the Citizen Lab"), in collaboration with First Department, Arjuna Team, and RESIDENT.ngo, have uncovered at least two separate spear-phishing campaigns targeting Russian and Belarusian nonprofit organizations, Russian independent media, international NGOs active in Eastern Europe, and at least one former U.S. ambassador. The Citizen Lab attributes one of the two campaigns to a known Russian threat group called COLDRIVER, with the other likely to be the work of a different, previously unnamed actor. Access Now and the Citizen Lab have dubbed this second actor "COLDWASTREL."

Spear phishing describes a highly personalized way of attacking victims, using carefully tailored information that aligns with a target's personal and professional experiences and activities. Based on Access Now and the Citizen Lab's assessment, it is likely that these threat actors or their sponsor organizations are still targeting civil society with spear phishing and other techniques. For more details on the Digital Security Helpline's investigation, read our full technical report.

READ THE FULL REPORT

// About COLDWASTREL

Our investigation into the first campaign began in March 2023, when Russian human rights organization First Department alerted us to a phishing email received by several international NGOs. The sender impersonated a staff member using the Proton Mail platform. First Department also reported that the same staff member's Proton Mail account had previously been targeted by a phishing attack in October 2022, resulting in them losing access to their account. In August 2024, we were again alerted by a previously targeted organization about a new phishing attack on their staff, which occurred in August 2024. Our Digital Security Helpline team investigated these cases, then reported them to Proton, ICANN, and other service providers.

While investigating the attacks, we discovered that an IP address used by the attacker was linked to domains impersonating several prominent civil society organizations active in Eastern Europe. We alerted the organizations in question, one of which confirmed they had received a similar phishing email, but preferred to stay anonymous for privacy and security reasons.

While some aspects of the attack indicate that the attacker, which we have dubbed "COLDWASTREL," may be acting in the interests of the Russian regime, we cannot confidently attribute the attack to a particular actor at this stage.

// About COLDRIVER

In early 2024, Access Now and the Citizen Lab identified a different cluster of phishing attacks. The organizations and individuals targeted in this campaign included Russian and Belarusian civil society organizations and independent media, international NGOs, and at least one former US ambassador. Citizen Lab has attributed this campaign to a Russia-based threat group COLDRIVER, also known as, among other names, STAR BLIZZARD, SEABORGIUM, and CALLISTO. You can read more about COLDRIVER in the Citizen Lab's investigation. According to several governments, this group is a subordinate of the Russian Federal Security Service (FSB)'s Centre 18.

// How the attacks were carried out

Below, we describe the pattern of the spear-phishing attacks we observed and offer guidance on how you can work to prevent or mitigate such attacks.

Both kinds of attacks were highly tailored to better deceive members of the target organizations. The most common attack pattern we observed was an email sent either from a compromised account or from an account appearing similar to the real account of someone the victim may have known. The phishing attacks were personalized to show scenarios that the individuals or their organizations might feasibly encounter in their daily work, mentioning topics such as event planning or financial discussions.

The attacks also typically included a seemingly locked PDF attachment, sometimes with a link purporting to help "unlock" the PDF's content, but which in fact led to fake login pages aimed at harvesting the target's information.

// The impact of the attacks

While some targets told us that they did not engage with the phishing emails described in the two attacks, others were deceived into entering their user credentials.

Even though we did not directly observe credentials being passed back to the attacker's infrastructure, it is likely that attackers were able to gain unauthorized access to some victims' email accounts.

If successful, such attacks could be enormously harmful, particularly to Russian and Belarusian organizations and independent media, since their email accounts are likely to contain sensitive information about their staff's identities, activities, relationships, and whereabouts. Any contact between Russian NGOs or independent media with Western-based organizations could be mischaracterized by the Russian government, and used as a pretext to designate them as a "foreign agent" or "undesirable organization." In some cases, this could even lead to individuals being criminally charged and imprisoned.

// How to protect yourself if you suspect you are being targeted

The following recommendations have been prepared jointly by Access Now and the Citizen Lab.

Start with prevention

Use two-factor authentication, correctly: Experts agree that setting up two-factor authentication (2FA) is one of the most powerful ways to protect your account from getting hacked.

However, hackers like COLDRIVER and COLDWASTREL may try to trick you into entering your second factor; we have seen attackers successfully compromise a victim who had enabled 2FA. People using SMS messaging as their second factor are also at greater risk of having their codes stolen if a bad actor takes over their phone account.

We recommend that people use more advanced 2FA options such as security keys or, if they are Gmail users, Google Passkeys. Here are three guides for increasing the level of security for your account:

- Get Google Passkeys (Google)

- How to: Enable two-factor authentication (Electronic Frontier Foundation)
- Set up multi factor authentication (Consumer Reports)
- Use a security key (Consumer Reports)

Enroll in programs for high-risk users. Google and some other providers offer optional programs for people who, because of who they are or what they do, may face additional digital risks. These programs not only increase the security of your account, but also flag to companies that you may face more sophisticated attacks. Such programs include:

- Google Advanced Protection
- Microsoft Account Guard
- Proton Sentinel

Received a message? Be a five-second detective

- **Step one: check your inbox for the sender's email.** Ask yourself if you have received messages from this account before. COLDRIVER often uses lookalike emails to impersonate people known to the target either personally or professionally, so you may see an email that appears to come from someone you know, writing about something you would expect them to write about. Even if you have received previous messages from the same email address, it is possible to "spoof" a familiar looking email address, so move on to the next step.
- **Step two: check with the sender over a different medium**. If you have any concerns or are at all suspicious, do not open any PDF attachment or click on any link sent in the email. Instead, check directly with the purported sender, via another service, to confirm whether or not they've reached out to you. If you don't already have direct contact with them, consider asking someone you trust to inquire on your behalf.
- **Step three: don't just click.** Always consult an expert before opening a document you are unsure about. If you want to view a document that you think is probably safe, but want to take care, open the file *within* your webmail. Google, Microsoft, and others open the files on their computers and display the contents to you. This protects you from malicious code embedded in a document. But it **will not prevent you from clicking on potentially malicious links inside the document.**
    - If you are viewing an attached document inside your webmail, you should remain careful. **Don't just click on any links**; copy and paste them into your browser before visiting. Examine the domain carefully: Is it what you would expect for the site you expect to be visiting? Advanced phishing kits are very good at impersonating popular services, and often the only visual clue that it is not the authentic site will be in the address bar of the browser.
    - If you see a "login page" pop up, **stop**. This is a good time to consult a trusted expert.
- **Step four: beware of "encrypted" or "protected" PDFs.** This kind of message is almost always a cause for concern. Legitimately encrypted PDFs almost never include a single "click here" button inside the PDF, and they don't show a blurred version of the contents. Never click on any "login" links or "buttons" inside a PDF you have been sent.

Considering online virus-checking sites? You may wish to use online virus-scanning sites such as VirusTotal or Hybrid Analysis to check suspicious links or files.

- These services offer a useful service and can be part of a good security practice, but they come with a very important caveat: **when you use such free services, you are not the customer, you are the product.** Your files are available to many researchers, companies, and governments.
- We do **not** recommend using such tools to check "sensitive" files that may contain personal information or other private topics. Instead, contact a trusted expert that can help.

Think you are being targeted?

These recommendations address the kind of phishing that COLDRIVER and COLDWASTREL are currently using, but there are many other ways you could be targeted. Whatever your level of risk, we encourage you to get personalized security recommendations from the Security Planner, which also maintains a list of emergency resources and advanced security guides.

If you suspect that you have already been targeted in an attack, reach out to a trusted practitioner for advice. It is crucial to evaluate any damage to your organization and/or to other related organizations and individuals, such as partners, participants, grantees, and others. If this is the case, keep them informed about what has happened, what has been leaked, how this may impact them, and what steps you are taking to mitigate this impact.

If you believe you have been compromised: Access Now's Digital Security Helpline is available to support members of civil society, including activists, media organizations, journalists, and human rights defenders, 24/7 in nine languages, including Russian.

- **Change your password right away**. If you are using the same password for other accounts, you should change the password for those accounts too. Consider using a password manager to keep track of multiple passwords.
- You can also review access logs on your accounts, such as Proton Mail's Authentication Logs, Gmail's Last Account Activity, and review devices with account access, as well as Microsoft's Check recent sign-in activity. Some users may still have questions after reviewing these logs. We encourage you to make a copy of the logs if you suspect you may have been targeted, to share with an expert for review.

NATALIA KRAPIVA

@natynettle

ACCESS NOW HELPLINE TEAM

@accessnow

SPEAR-PHISHING CASES FROM EASTERN EUROPE IN 2022-2024: A TECHNICAL BRIEF

accessnow

Access Now defends and extends the digital rights of people and communities at risk. As a grassroots-to-global organization, we partner with local actors to bring a human rights agenda to the use, development, and governance of digital technologies, and to intervene where technologies adversely impact our human rights. By combining direct technical support, strategic advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

This paper is an Access Now publication. It is written by **Access Now's Digital Security Helpline team.** We would like to thank Natalia Krapiva, Senior Tech Legal Counsel at Access Now, who provided support for this brief. For more information, please visit: **https://www.accessnow.org**

Contact: **Hassen Selmi** | Incident Response Lead
hassen@accessnow.org

Published in August 2024

Spear-phishing cases from Eastern Europe in 2022-2024: a technical brief

In this technical brief, Access Now's Digital Security Helpline ("the Helpline") outlines forensic evidence for spear-phishing campaigns targeting civil society members from Eastern Europe and international NGOs working in the region. The analysis covers two separate campaigns documented between October 2022 and August 2024.

Our work highlights the key similarities between the campaigns, as well as their differences. The combination of the attack modalities, the profile of the victims, and other technical evidence points to the perpetrators being threat actors close to the Russian regime. The Citizen Lab at the Munk School of Global Affairs & Public Policy at the University of Toronto ("the Citizen Lab") has confirmed that the attacks Access Now observed between April and June 2024 could be attributed to COLDRIVER. We also identified another cluster of attacks between October 2022 and August 2024 that were likely the work of a different actor, who does not appear to have been named previously and who we refer to as COLDWASTREL. We hope that the information provided will support civil society in raising awareness of the risks, further safeguarding their communications, and exercising further caution if they have a higher risk profile.

Additional context can be found in Access Now's blog post, "*Caught on the net: Russia-linked phishing campaigns ensnare Russian and Belarusian civil society, as well as international NGOs*."

Key findings

- Two spear-phishing campaigns targeted members of civil society from Eastern Europe and international NGOs working in the region. The campaigns are the work of two different threat actors, COLDRIVER and COLDWASTREL.
- The attacks used Proton Mail email addresses to impersonate organizations or individuals that were familiar or known to the victims.
- The attacks used PDF documents that appeared locked and provided a malicious link purporting to unlock them, but which instead led to fake login pages.
- The attacks were intended to mimic everyday scenarios regularly encountered by the targeted organizations, which work to defend and uphold human rights, thus underscoring the highly targeted nature of the campaign.

Campaign A: attacks by novel threat actor COLDWASTREL

A first set of attacks documented by the Helpline between October 2022 and August 2024 was likely the work of a threat actor that Access Now and the Citizen Lab have dubbed "COLDWASTREL."

The Helpline was first alerted to these attacks in March 2023. We learned that an unknown threat actor was using a Proton Mail address to impersonate a member of staff at a prominent Russian civil society organization, sending well-crafted emails to targets, including international NGOs.

The emails employed by the threat actor were designed to appear to come from an account well-known to the targets, modifying only one character to deceive those who would notice less subtle phishing attempts.

The modified characters were also carefully chosen to further dissimulate the deception. For example, the attacker replaced "s" with "c" before "k," which deflects attention both through use of phonetics and the similar physical appearance of the names when typed out.

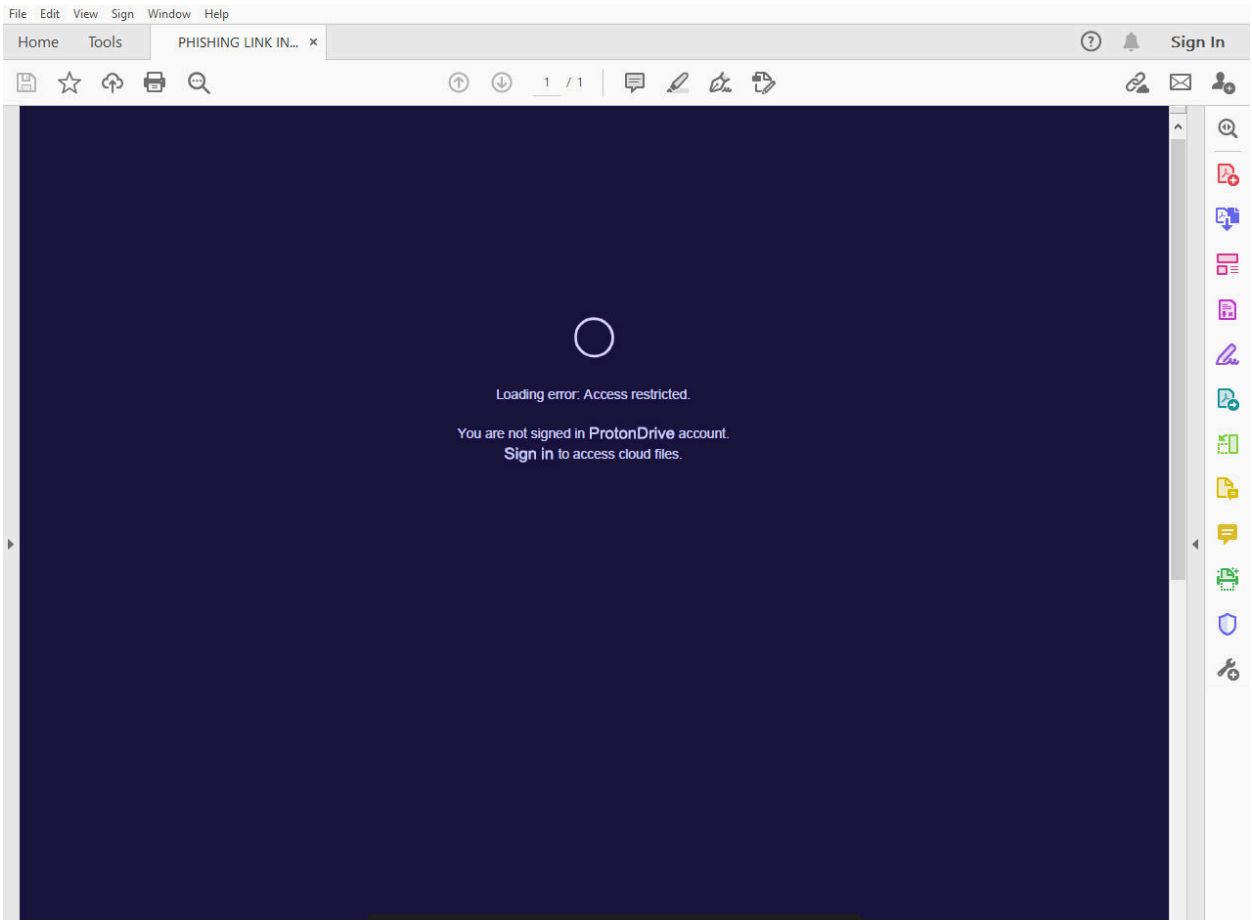
Here's an example, using a pseudonym:

> A real email address: Ivan.le**s**kovic@protonmail.com
>
> A fake address used: Ivan.le**c**kovic@protonmail.com

The person whose account was impersonated in this manner was also targeted by a phishing attempt against their email that resulted in them losing access to their account. We believe that COLDWASTREL was also behind this attack.

Subsequent attacks in 2023 employed an alternative tactic. Attackers created a mail server with fake domains to impersonate an existing organization, including victims' actual partners and acquaintances. They combined this method with the use of aliases to appear familiar to the victims, using the one-character change method described above to deflect possible suspicion and make the attack harder to detect.

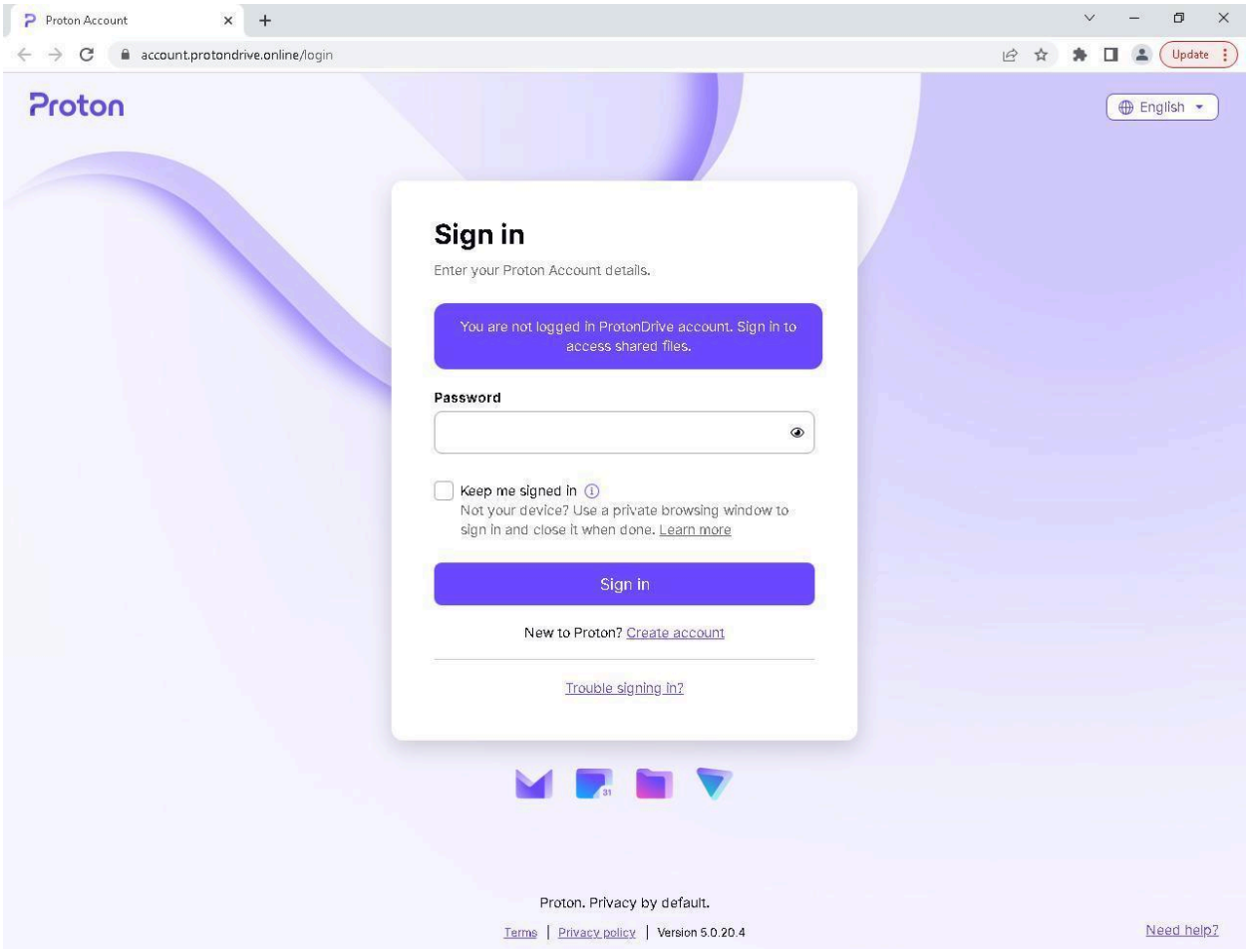
In some of the cases analyzed, the emails contained a PDF attachment which appeared to be locked. The same emails provided a link that purported to help unlock the PDF (see screenshot below).



Sample of a PDF preview presented to targets as part of the COLDWASTREL campaign.

When followed, the link led to a fake Proton Mail login page. The Helpline was unable to verify any working links, as these appeared to have either been disabled or to have expired at the moment of analysis. However, in some cases, the fake login pages seemed able to harvest passwords and codes for two-factor authentication from the victims.

As a reference, see the screenshot below, shared by one victim, which includes a fake URL at the top (account.protondrive[.]online/login):



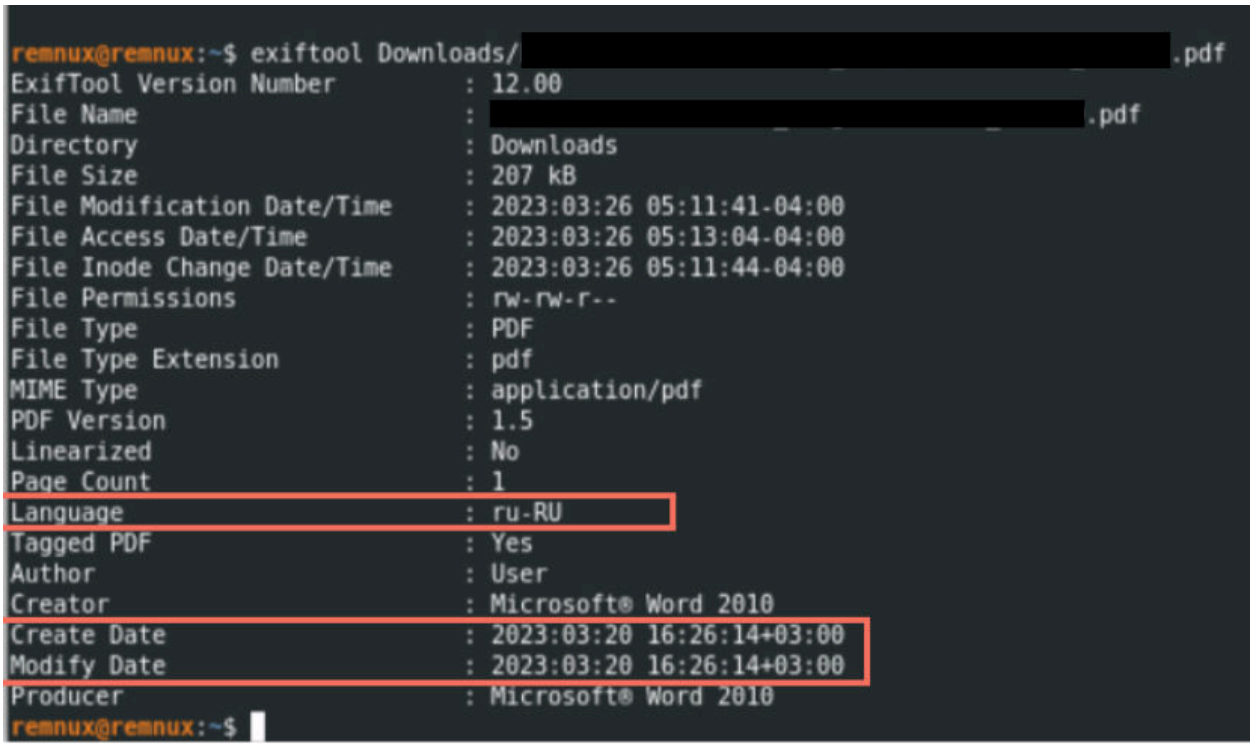
Sample of fake Proton Mail login page presented to targets as part of COLDWASTREL campaign.

Attackers' use of virtual private servers allowed the Helpline to identify and alert additional victims

By finding the virtual private servers that attackers employed in 2023 to host fake pages and email servers, the Helpline was able to identify other potential victims beyond those who initially sought our assistance, and to reach out proactively to alert them about the risk. At least one international human rights organization supporting civil society in the region confirmed that their staff were targeted with a similar campaign, although they did not share further details for analysis by the Helpline.

The Helpline believes that the threat actors behind this spear phishing campaign may be aligned with or close to the Russian regime. The victims are involved in human rights work in Russia, Ukraine, and across the region, which makes them of interest to the Kremlin. The attackers used context from activities that are highly relevant to the targets' work, such as references to funding and grant proposals. This reveals a profound understanding of the regional context and the targets' work, and a highly personalized attempt to exploit their vulnerabilities.

In addition, the analysis of the metadata included in the PDF documents deployed in the COLDWASTREL attacks showed the time of creation to have been GMT+3 (Moscow time) and the language to be ru-RU (Russian), as shown below. It should be noted that it is not definitive proof that the attackers are connected with Russia, since any attacker can change their computer time and language.



Output of exiftool shows a 2023 malicious PDF file creation time, time zone (GMT+3), and the system language (ru-RU).

While some aspects of the attack indicate that COLDWASTREL may be acting in the interests of the Russian regime, we cannot confidently attribute the attack to any particular actor.

Readers should note that while finalizing this technical brief, we were alerted by one of the organizations previously targeted about a new phishing attack on their staff, which occurred in August 2024. Citizen Lab has tentatively concluded that COLDWASTREL is likely also the threat actor behind this latest attack.

Campaign B: attacks the Citizen Lab attributes to COLDRIVER

The spear-phishing campaign we observed in 2024 has some similarities with campaign A, such as reaching out to organizations working in Eastern Europe with a PDF containing malicious links.

The attackers also attempted to impersonate people that the victims knew, but this time, with mixed results. Some of the victims were suspicious about the communications received, recalling, for example, that they had not shared their contact details with the contact being impersonated, nor did the real contact have a Proton Mail address.

Sample of the PDF preview presented to the targets as part of the COLDRIVER campaign.

The Helpline noted several other key differences in attackers' tactics and techniques. The attackers in the cases we observed between April and June 2024 used virtual private servers with Hostinger International Limited as their preferred host provider. However, we did not see any use of fake domains purporting to belong to real organizations, and we only analyzed instances where the attackers used Proton Mail email addresses to deliver their attacks. This made it harder to identify other potential victims compared with campaign A, for instance.

In addition, the links embedded in the campaign B PDF files included different mechanisms for validation, which is the process through which the code collects data from the target device, sends it to the server for processing, and offers different responses depending on what is analyzed.

When Helpline analysts first visited these links, they observed an obfuscated code:

The JavaScript machine validation code is obfuscated using Hunter PHP Javascript Obfuscator.

The deobfuscation of this code shows an initial step, using a validation code, to check the victim's machine type, before delivering the web content. If the machine fails this check, the visitor is redirected to a generic landing page or to a Captcha page, which are clearly not harmful. This technique is used as an attempt to limit analysis and to allow only the malicious code to be served to the intended target.

```
function handleResponse(res) {
    switch (res.type) {
    case 'error':
        hcaptcha.render('captcha-1', {
            sitekey: 'af5a26f0-15c2-4c9e-bf82-53b0a8c81da2',
            theme: 'light',
            'error-callback': 'onError',
            callback: 'onSuccess'
        });
        break;
    case 'death':
        window.location.href = '/';
        break;
    case 'success':
        window.location.replace(res.url);
        break;
    }
}
```

Part of the deobfuscated code showing the function responsible for redirecting users based on the malicious server response.

Unfortunately, the Helpline could not proceed to the next stage of the validation or determine whether or not it succeeded. The code that determines the page's response is implemented inside a PHP file on the server side, which was inaccessible to analysts. The second stage could be either a fake login page, as used in the COLDWASTREL attacks, or a link to download malware.

The PDF samples from this campaign did not contain create or modify dates. The language was set as en-US (English) and the attackers used Western-sounding names for the author metadata. It is possible that the metadata was removed to avoid leaving traces that could be used for attribution.

The attack victims were Russian and Belarusian NGOs and independent media. The sharing of seemingly locked PDF files, along with links to "unlock" them, mirrors the strategy of attacks documented by Google's Threat Analysis Group (TAG), which they attribute to Russian threat actor COLDRIVER and which is confirmed by the Citizen Lab's analysis.

Conclusion: remain on high alert

While the attacks outlined in this report are not technically sophisticated, they rely on sophisticated social engineering methods in addition to techniques, such as the use of machine validation, omitting PDF metadata, and use of private hosting. These are measures that the attackers chose to reduce any detection surface.

The threat from these spear-phishing attacks remains high for civil society and journalists who are working to defend human rights with a focus on Russia and Eastern European countries. The main safeguard for them is high awareness of the risks, as well as careful treatment of all communications received.

The following recommendations have been prepared jointly by Access Now and the Citizen Lab.

Start with prevention

Use two-factor authentication, correctly: Experts agree that setting up two-factor authentication (2FA) is one of the most powerful ways to protect your account from getting hacked.

However, hackers like COLDRIVER and COLDWASTREL may try to trick you into entering your second factor; we have seen attackers successfully compromise a victim who had enabled 2FA. People using SMS-messaging as their second factor are also at greater risk of having their codes stolen if a bad actor takes over their phone account.

We recommend that people use more advanced 2FA options such as security keys or, if they are Gmail users, Google Passkeys. Here are three guides for increasing the level of security for your account:

- Get Google Passkeys (Google)
- How to: Enable two-factor authentication (Electronic Frontier Foundation)
- Set up multi factor authentication (Consumer Reports)

- Use a security key (Consumer Reports)

Enroll in programs for high-risk users. Google and some other providers offer optional programs for people who, because of who they are or what they do, may face additional digital risks. These programs not only increase the security of your account, but also flag to companies that you may face more sophisticated attacks. Such programs include:

- Google Advanced Protection
- Microsoft Account Guard
- Proton Sentinel

Received a message? Be a five-second detective

- **Step one: check your inbox for the sender's email.** Ask yourself if you have received messages from this account before. COLDRIVER often uses lookalike emails to impersonate people known to the target either personally or professionally, so you may see an email that appears to come from someone you know, writing about something you would expect them to write about. Even if you have received previous messages from the same email address, it is possible to "spoof" a familiar looking email address, so move on to the next step.
- **Step two: check with the sender over a different medium**. If you have any concerns or are at all suspicious, do not open any PDF attachment or click on any link sent in the email. Instead, check directly with the purported sender, via another service, to confirm whether or not they've reached out to you. If you don't already have direct contact with them, consider asking someone you trust to inquire on your behalf.
- **Step three: don't just click.** Always consult an expert before opening a document you are unsure about. If you want to view a document that you think is probably safe, but want to take care, open the file *within* your webmail. Google, Microsoft, and others open the files on their computers and display the contents to you. This protects you from malicious code embedded in a document. But it **will not prevent you from clicking on potentially malicious links inside the document.**
    - If you are viewing an attached document inside your webmail, you should remain careful. **Don't just click on any links**; copy and paste them into your browser before visiting. Examine the domain carefully: Is it what you would expect for the site you expect to be visiting? Advanced phishing kits are very good at impersonating popular services, and often the only visual clue that it is not the authentic site will be in the address bar of the browser.
    - If you see a "login page" pop up, **stop**. This is a good time to consult a trusted expert.
- **Step four: beware of "encrypted" or "protected" PDFs.** This kind of message is almost always a cause for concern. Legitimately encrypted PDFs almost never include a single "click

here" button inside the PDF, and they don't show a blurred version of the contents. Never click on any "login" links or "buttons" inside a PDF you have been sent.

Considering online virus-checking sites? You may wish to use online virus-scanning sites such as VirusTotal or Hybrid Analysis to check suspicious links or files.

- These services offer a useful service and can be part of a good security practice, but they come with a very important caveat: **when you use such free services, you are not the customer, you are the product.** Your files are available to many researchers, companies, and governments.
- We do **not** recommend using such tools to check "sensitive" files that may contain personal information or other private topics. Instead, contact a trusted expert that can help.

Think you are being targeted?

These recommendations address the kind of phishing that COLDRIVER and COLDWASTREL are currently using, but there are many other ways you could be targeted. Whatever your level of risk, we encourage you to get personalized security recommendations from the Security Planner, which also maintains a list of emergency resources and advanced security guides.

If you suspect that you have already been targeted in an attack, reach out to a trusted practitioner for advice. It is crucial to evaluate any damage to your organization and/or to other related organizations and individuals, such as partners, participants, grantees, and others. If this is the case, keep them informed about what has happened, what has been leaked, how this may impact them, and what steps you are taking to mitigate this impact.

If you believe you have been compromised: Access Now's Digital Security Helpline is available to support members of civil society, including activists, media organizations, journalists, and human rights defenders, 24/7 in nine languages, including Russian.

- **Change your password right away**. If you are using the same password for other accounts, you should change the password for those accounts too. Consider using a password manager to keep track of multiple passwords.
- You can also review access logs on your accounts, such as Proton Mail's Authentication Logs, Gmail's Last Account Activity, and review devices with account access, as well as Microsoft's Check recent sign-in activity. Some users may still have questions after reviewing these logs. We encourage you to make a copy of the logs if you suspect you may have been targeted, to share with an expert for review.

Annex: Selected indicators of compromise (some omitted for privacy and security reasons)

COLDWASTREL

Domains:

protondrive[.]online
service-proton[.]me
protondrive[.]me
protondrive[.]services

VPSes used:

185.247.224[.]39 (observed in the first quarter of 2023)
194.36.189[.]125 (observed in the third to fourth quarter of 2022)
91.196.70[.]47 (observed in the second quarter of 2023 to first quarter of 2024)
46.246.1[.]187 (observed in the first to second quarter of 2024)
38.180.86[.]201 (observed in the second to third quarter of 2024)
38.180.18[.]66 (observed in the second to third quarter of 2024)

PDF Samples:

4a9a2c2926b7b8e388984d38cb9e259fb4060cccc2d291c7910be030ae5301a3
a2bfc72714978a1b025717d8028168e91ebb10eeb576cd047990e960442c25ce
751496922cef7592d7bef6eff075c2531971a778d56bce50e1217bcdccabdd5b

COLDRIVER

Domains:

egenre[.]net
eilatocare[.]com
xsltweemat[.]org

PDF Samples:

0ded441749c5391234a59d712c9d8375955ebd3d4d5848837b8211c6b27a4e88
b07d54a178726ffb9f2d5a38e64116cbdc361a1a0248fb89300275986dc5b69d
00664f72386b256d74176aacbe6d1d6f6dd515dd4b2fcb955f5e0f6f92fa078e

Rivers of Phish

Sophisticated Phishing Targets Russia's Perceived Enemies Around the Globe

By John Scott-Railton (https://citizenlab.ca/author/jsrailton/)[1], Rebekah Brown (https://citizenlab.ca/author/rbrown/)[2], Ksenia Ermoshina (https://citizenlab.ca/author/kermoshina/), and Ron Deibert (https://citizenlab.ca/author/profd/)

[1] Co-lead author [2] Co-lead author

August 14, 2024

Summary

- A sophisticated spear phishing campaign has been targeting Western and Russian civil society.
- This campaign, which we have investigated in collaboration with Access Now and with the participation of numerous civil society organizations including First Department (https://dept.one/), Arjuna Team, and RESIDENT.ngo (https://resident.ngo/), engages targets with personalized and highly-plausible social engineering in an attempt to gain access to their online accounts.
- We attribute this campaign to COLDRIVER (also known as Star Blizzard, Callisto and other designations). This threat actor is attributed to the Russian Federal Security Service (FSB) by multiple governments.
- We identified a second threat actor targeting similar communities, whom we name COLDWASTREL. We assess that this actor is distinct from COLDRIVER, and that the targeting that we have observed aligns with the interests of the Russian government.
- The Citizen Lab is sharing all indicators with major email providers to assist them in tracking and blocking these campaigns.

Click here (https://www.accessnow.org/russian-phishing-campaigns/) to read the Access Now Report and the Access Now Helpline Technical Brief. (https://www.accessnow.org/russian-phishing-technical-brief)

1. River of Phish: Campaign Overview

Our collaborative investigation with Access Now (https://www.accessnow.org/), with the assistance of multiple additional civil society organizations including First Department (https://dept.one/), Arjuna Team, and RESIDENT.ngo (https://resident.ngo/), has identified digital targeting using sophisticated spear phishing by this threat actor across multiple countries and sectors within civil society.

Observed Targets

The targets range from prominent Russian opposition figures-in-exile to staff at nongovernmental organizations in the US and Europe, funders, and media organizations. A focus on Russia, Ukraine, or Belarus is a common thread running through all of the cases. Some of the targets still live and work in Russia, placing them at considerable risk. Almost all targets that spoke with us and our investigative partner, Access Now, have chosen to remain unnamed and, for their privacy and safety, we are only including indicators from a limited selection of the cases that we have examined.

Polina Machold, Publisher of Proekt Media (https://www.proekt.media/en/home/) is among the targets, and we observed the attackers masquerading as an individual known to her. Proekt conducts high profile investigative reporting into official corruption and abuses of power in Russia. They are well known for high-profile reporting on Vladimir Putin, Ramzan Kadyrov, and other highly-placed Russian officials. Soon after their reporting into Russia's interior minister in 2021, they were declared (https://rsf.org/en/proekt-first-russian-media-outlet-be-declared-undesirable) an "undesirable organization" by the Russian Government.

We have also observed targeting of former officials and academics in the US think tank and policy space. For example, former US Ambassador to Ukraine, Steven Pifer was targeted with a highly-credible approach impersonating someone known to him: a fellow former US Ambassador.

We judge that these targets may have been selected for their extensive networks among sensitive communities, such as high-risk individuals within Russia. For some, successful compromise could result in extremely serious consequences, such as imprisonment or physical harm to themselves or their contacts.

Importantly, we suspect that the total pool of targets is likely much larger than the civil society groups whose cases we have analyzed. We have observed US government personnel impersonated as part of this campaign, and given prior reporting about COLDRIVER's targeting, we expect the US government remains a target.

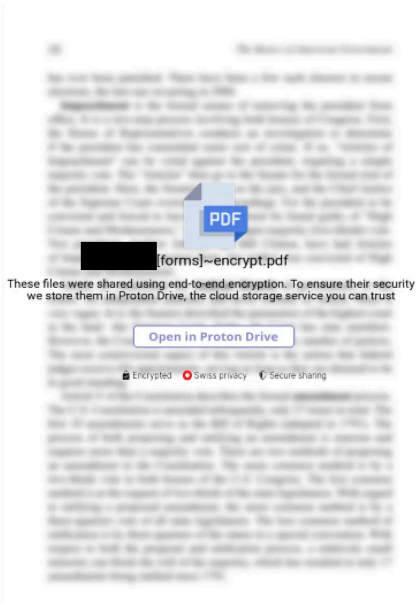
Typical Attack Flow: A Credible, Personalized Approach

The most common tactic we have observed is for the threat actor to initiate an email exchange with the target masquerading as someone known to them. This tactic includes masquerading as colleagues, funders, and US government employees. Typically, the messages contain text requesting that the recipient review a document relevant to their work, such as a grant proposal or an article draft.

In some cases, we have observed additional communication by the threat actor preceding or following the targeting message. Often highly and effectively personalized, this communication illustrates the depth of the threat actors' understanding of the targets. Multiple targets believed that they were exchanging emails with a real

person.

We often observed the attacker omitting to attach a PDF file to the initial message requesting a review of the "attached" file. We believe this was intentional, and intended to increase the credibility of the communication, reduce the risk of detection, and select only for targets that replied to the initial approach (e.g. pointing out the lack of an attachment).



(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2024/08/image8.png&nocache=1)

Figure 1: Screenshot of a purportedly-encrypted PDF lure. The phishing page is reached by clicking. (The screenshot has been slightly redacted to remove the name of an impersonated organization).

The email message typically contains an attached PDF file purported to be encrypted or "protected," using a privacy-focused online service such as ProtonDrive, for example. In fact, this is a ruse. When opened, the PDF displays what appears to be blurred text along with a link to "decrypt" or access the file. Actual ProtonDrive encryption looks substantially different (https://proton.me/support/send-large-files-proton-drive) from the River of Phish lures, suggesting that the attackers are relying on a general lack of awareness of what secure and encrypted document sharing looks like. In other cases, the blurred PDF includes text saying that a preview is not available, again soliciting a click.

While typical attacks were limited to a PDF, we also observed a few cases in which the attackers also sent an email crafted to appear as a document share, with the phishing link directly embedded in the email message. When one such case seemingly failed to generate a successful compromise, the attackers followed up with a PDF.

In some cases, the attackers followed up with targets that failed to enter their credentials with multiple messages asking if they had seen or "reviewed" the material. This approach, again, suggests a high degree of focus on particular targets.

If the Target Clicks

If the target clicks on the link, their browser will fetch JavaScript code from the attacker's server that computes a fingerprint of the target's system and submits it to the server (see: *Target Fingerprinting*). If the server elects to proceed with the attack, the server will return a URL, and the JavaScript code running in the target's browser will redirect the target there. If the server chooses, a CAPTCHA (from hCaptcha (https://www.hcaptcha.com/)) may be shown to the user prior to any redirect. The URL to which the target is redirected is typically a webpage crafted by the attacker to look like a genuine login page for the target's email service (e.g. Gmail or ProtonMail).

The login page may be pre-populated with the target's email address to mimic the legitimate login page. If the target enters their password and two-factor code into the form, these items will be sent to the attacker who will use them to complete the login and obtain a session cookie for the target's account. This cookie allows the attacker to access the target's email account as if they were the target themselves. The attacker can continue to use this token for some time without re-authenticating.

The use of a credible email ruse plus a PDF containing a phishing link is a favorite technique of multiple threat actors. Notably, PDF viewers built into webmail services like Gmail allow the recipient to click on hyperlinks within a PDF, and thus do not impede this attack.

2. River of Phish Campaign Infrastructure

First-Stage Domains

The first-stage infrastructure for this campaign involves phishing links embedded in the delivered PDFs, or sent in emails crafted to appear as document shares. The attackers typically register the domains and host the websites using Hostinger (https://www.hostinger.com/). Domains registered with Hostinger are hosted on shared servers which rotate IP addresses approximately every 24 hours, making the campaign more difficult to track. We did not identify any cases where a domain was operationally used within 30 days of its registration. This is a possible attempt to avoid being blocked by detection rules aimed at flagging emails or attachments with hyperlinks containing a recently registered domain.

Domain	Registration date	Date of Phishing email	Registrar	TLS Issuer
ithostprotocol[.]com	2024-01-16	2024-02-20	NameCheap	cPanel
xsltweemat[.]org	2024-03-14	2024-04-12	Hostinger	Let's Encrypt
eilatocare[.]com	2024-04-09	2024-05-29	Hostinger	Let's Encrypt
egenre[.]net	2024-05-19	2024-06-19	Hostinger	Let's Encrypt
esestacey[.]net	2024-05-19	2024-06-19	Hostinger	ZeroSSL
ideaspire[.]net	2024-05-20	2024-06-24	Hostinger	Let's Encrypt

Table 1: Examples of first-stage domains used in this campaign.

If the target clicks on the link in the PDF, the attack moves onto the next stage, which involves fingerprinting the user's system.

Target Fingerprinting

Each first-stage domain runs JavaScript code to fingerprint the target's browser and returns the fingerprint to the server, which decides how to proceed. Because we cannot see the server's code, we are not fully sure what the purpose of the fingerprinting is. However, because the server can elect to show a CAPTCHA to the target, we presume that the purpose of the fingerprinting may be to prevent certain automated tools from obtaining or analyzing the second-stage infrastructure, which contains the phishing page.

We did not directly observe the second stage of the attack or the credentials being passed back to the attacker's infrastructure; however, based on the targets' descriptions of the login page it is likely that the attackers leveraged a tool that is specifically designed to capture user credentials and enable unauthorized access, such as Evilginx (https://github.com/kgretzky/evilginx2) or another phishing platform. We note that COLDRIVER has been observed using Evilginx (https://www.microsoft.com/en-us/security/blog/2023/12/07/star-blizzard-increases-sophistication-and-evasion-in-ongoing-attacks/) in recent cases.

Our investigative partner, Access Now, has included a description of the fingerprinting code in their Technical Brief (https://www.accessnow.org/russian-phishing-technical-brief). The fingerprinting code was obfuscated using the Hunter PHP Javascript Obfuscator, a tool that is publicly available on GitHub (https://github.com/nicxlau/hunter-php-javascript-obfuscator).

Frequent Metadata Overlaps Across PDFs

PDFs associated with this campaign share consistent characteristics, including the location and formatting of the malicious link within the PDF, the PDF metadata, and the use of a fake English-language name that is different in each case for the PDF author. Based on the names identified in the PDFs, it appears that a name list such as this one (https://github.com/marcotcr/checklist/blob/master/checklist/data/names.json) or this one (https://github.com/FinNLP/humannames/blob/master/list.txt) was used in the generation of these names.

The chart below includes metadata from some PDFs that were shared directly with The Citizen Lab and Access Now.

A Selection of PDFs from the River of Phish Campaign

SHA256	Author Name	Producer	Lan
b07d54a178726ffb9f2d5a38e64116cbdc361a1a0248fb89300275986dc5b69d	Gracelyn Reilly	LibreOffice 7.0	en
0ded441749c5391234a59d712c9d8375955ebd3d4d5848837b8211c6b27a4e88	Talon Blackburn	LibreOffice 7.0	en
efa2fd8f8808164d6986aedd6c8b45bb83edd70ca4e80d7ff563a3fbc05eab89	Howard Howe	LibreOffice 7.0	en
384d3027d92c13da55ceef9a375e8887d908fd54013f49167946e1791730ba22	Annabelle Kline	LibreOffice 7.0	en
00664f72386b256d74176aacbe6d1d6f6dd515dd4b2fcb955f5e0f6f92fa078e	Paulina Mullen	LibreOffice 7.0	en
79f93e57ad6be28aae62d14135140289f09f86d3a093551bd234adc0021bb827	Emery Hogan	LibreOffice 7.0	en

Table 2: Examples of metadata details on malicious PDFs.

Target Phishing

In the cases we analyzed as part of this particular campaign, user credentials and associated two-factor authentication (2FA) tokens appear to be the primary targets of this phase of attack. We did not find any spyware delivered to target devices as part of this particular campaign. The focus on account access simplifies the attack infrastructure that is needed, as the attackers do not need to gain persistence or establish ongoing communications with the target's machine. It is important to note that the individuals and organizations targeted in this campaign likely face additional threats, such as spyware attacks (See here (https://citizenlab.ca/2024/05/pegasus-russian-belarusian-speaking-opposition-media-europe/), for example).

In January of 2024, Google's Threat Analysis Group (TAG) reported (https://blog.google/threat-analysis-group/google-tag-coldriver-russian-phishing-malware/) on a custom malware backdoor called SPICA, which they assessed was the first known case of COLDRIVER developing and deploying custom malware. Similarly, we believe some of the targets who shared files with us may be regularly targeted by multiple threat actors and using multiple Tactics, Techniques, and Procedures (TTPs (https://www.splunk.com/en_us/blog/learn/ttp-tactics-techniques-procedures.html)). While this particular campaign did not leverage malware, we encourage human rights defenders, dissidents, journalists, and other members of civil society that may be targeted by Russian authorities to exercise extreme vigilance and contact experts such as Access Now's Digital Security Helpline (https://www.accessnow.org/help/) for help. We provide tips on how to identify suspicious communications below (See: *Protect Yourself & Your Colleagues*).

3. River of Phish: COLDRIVER Attribution

COLDRIVER is a Russia-based threat group attributed by several (https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet#fsb-centre-18) governments (https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-341a) to be subordinate to the Russian Federal Security Service (FSB) Centre 18 (*See: The Russian Cyber Espionage Landscape*, below). They have been active since at least 2019, possibly earlier, and their tactics primarily include very-involved social engineering and persona development. These personas are typically used to trick the target into visiting a malicious link, leading to the theft of their credentials, the bypassing of 2FA, and access to the target's information. This group has targeted widely in a pattern that aligns with Russian state interests, including targeting academia, NGOs, government institutions, and think tanks.

Selected Prior Reporting on COLDRIVER

Prior reporting on COLDRIVER describes strikingly similar tactics to the ones we see in this campaign. In 2017, cybersecurity firm F-Secure reported (https://web.archive.org/web/20170417102235/https://www.f-secure.com/documents/996508/1030745/callisto-group) on the activities of a group they tracked as "*Callisto group*", writing that they had tracked them since 2015. Their research highlighted the group's use of spear phishing (https://www.bbc.com/news/technology-39588703) to target "military personnel, government officials, think tanks and journalists." The attackers frequently impersonated legitimate websites and email addresses to trick targets into providing their credentials. At the time, F-Secure did not publicly attribute the group.

Company	Name assigned
F-Secure	Callisto group

Company	Name assigned
Microsoft	Star Blizzard / SEABORGIUM
Google TAG	COLDRIVER
PWC	Blue Callisto
Proofpoint	TA446
Sekoia	Calisto
Recorded Future	Blue Charlie
Mandiant	UNC4057

Table 3: One Threat Actor, Many Codenames.

In 2022, Microsoft reported on the group (https://www.microsoft.com/en-us/security/blog/2022/08/15/disrupting-seaborgiums-ongoing-phishing-operations/), which they track as *Star Blizzard* (previously *SEABORGIUM*). Google's Threat Assessment Group (TAG) (https://blog.google/threat-analysis-group/tracking-cyber-activity-eastern-europe/) reported on them as *COLDRIVER*, PWC reported (https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/blue-callisto-orbits-around-us.html#footnotes) on them as *Blue Callisto,* Proofpoint reported on them as TA446 (https://x.com/proofpoint/status/1618657863874015233), Sekoia reported (https://blog.sekoia.io/calisto-show-interests-into-entities-involved-in-ukraine-war-support/) on them as *Calisto,* and Recorded Future reports on them as *Blue Charlie*. All research teams described similar tactics: elaborate spear phishing campaigns impersonating individuals known to the targets with the goal of stealing credentials to accounts and accessing sensitive information. In 2022, attribution was typically framed as "a likely Russia-based actor (https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/blue-callisto-orbits-around-us.html)."

Attribution of COLDRIVER to the FSB in a Joint Governmental Advisory

In December 2023, government agencies from Australia, Canada, New Zealand, the United Kingdom, and the United States issued a joint cybersecurity advisory (https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-341a) detailing the activities of COLDRIVER. The advisory attributed the group to the FSB's Centre 18. The advisory notes that COLDRIVER's targets include "academia, defense, governmental organizations, NGOs, think tanks and politicians." The TTPs outlined in the advisory include extended target reconnaissance, the use of fake email and social media accounts, preference to target personal emails, the use of conference or event invitations as lures, the use of malicious domains impersonating legitimate organizations and more.

Attributing The River of Phish Campaign to COLDRIVER

Multiple TTPs and targeting from the River of Phish campaign closely align with public reporting on COLDRIVER. However, some of COLDRIVER's tactics (like lures using "encrypted" documents) share certain similarities with other threat actors. To increase our confidence, we sought to ensure that the River of Phish campaign matches multiple other research groups' COLDRIVER attribution. To that end, we approached Microsoft MSTIC, Proofpoint, and PwC, among others. Materials they shared enabled us to identify multiple direct overlaps be-

tween the River of Phish campaign and COLDRIVER. Finally, each independently confirmed that the activity we identified matched their own tracking of COLDRIVER. Together, this information suggests that the River of Phish campaign is attributable to the threat actor identified as COLDRIVER.

River of Phish Sample Overlap with Known COLDRIVER Campaigns

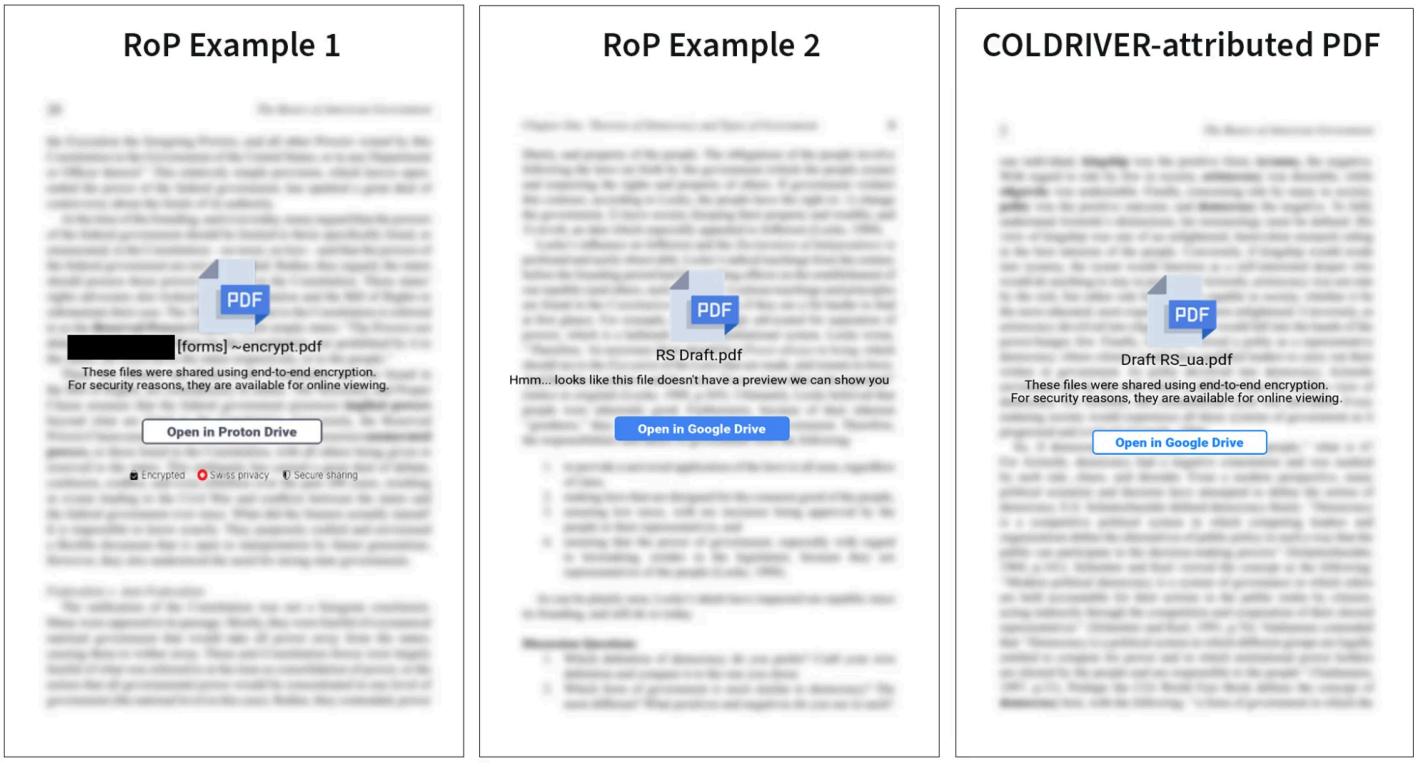
Proofpoint shared several publicly-available PDFs (on VirusTotal) with us that they attribute to COLDRIVER. Examination of these PDFs yielded multiple critical overlaps with the River of Phish campaign including: (a) matching bait PDF document structure and metadata and (b) overlapping phishing infrastructure.

Like the River of Phish ("RoP") PDFs (See: Table 2 above), those shared by Proofpoint included identical LibreOffice versions, seemingly-randomized author names, and en-US language settings.

Publicly-Available PDFs identified by Proofpoint as COLDRIVER			
c1fa7cd73a14946fc760a54ebd0c853fab24a080cbf6b8460a949f28801e16fc	Alexis Hill	LibreOffice 7.0	en-US
603221a64f2843674ad968970365f182c228b7219b32ab3777c265804ef67b0a	Carley Rivers	LibreOffice 7.0	en-US
df9d77f3e608c92ef899e5acd1d65d87ce2fdb9aab63bbf58e63e6fd6c768ac3	Haylie Wolf	LibreOffice 7.0	en-US

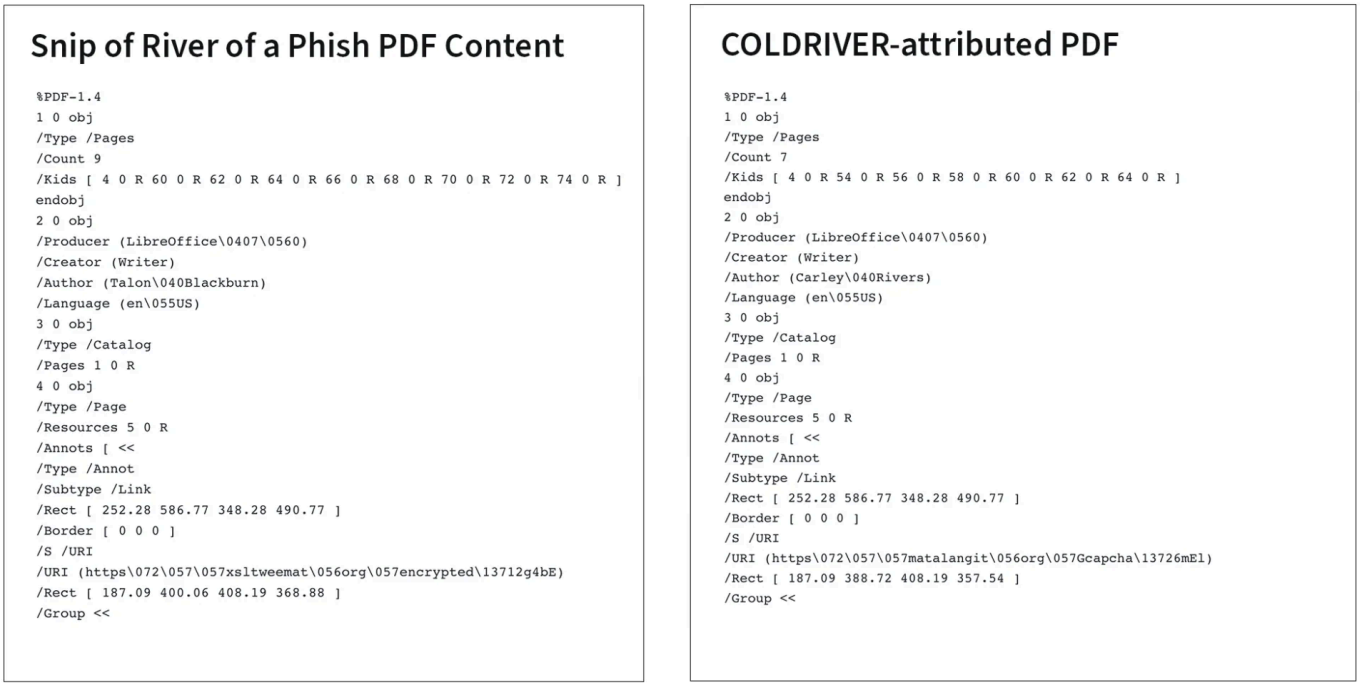
Table 4: Publicly-available COLDRIVER PDFs.

In addition to the PDF document metadata overlap, we observed substantial visual and content similarities in the PDFs. For example, RoP Example 1 shares bait text with this COLDRIVER-attributed text, and RoP Example 2 includes a variant on the filename used in the COLDRIVER-attributed PDF (See: Figure 2).



(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2024/08/stitched-figure6-1.png&nocache=1)

Figure 2: Two River of Phish PDFs and one COLDRIVER PDF (Note: The Example 1 screenshot has been redacted to remove the name of an impersonated organization).



(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2024/08/stitched-figure7.png&nocache=1)

Figure 3: Comparing River of Phish and COLDRIVER PDF content.

Phishing Infrastructure Overlaps

In addition to the highly similar PDF content, phishing infrastructure linked from RoP bait PDFs showed substantial overlaps between the RoP campaign and COLDRIVER. The COLDRIVER-attributed PDFs contained links to multiple phishing domains (For example, See: Table 5).

Domain	Registration date	Registrar	TLS Issuer
togochecklist[.]com	2023-08-28	NameCheap	Let's Encrypt
vocabpaper[.]com	2024-03-15	Hostinger	Let's Encrypt
matalangit[.]org	2024-05-07	Hostinger	ZeroSSL

Table 5: Domain registration patterns and TLS issuers for known COLDRIVER PDFs.

The COLDRIVER phishing domain registration patterns exhibited similar characteristics to the ones we identified, such as registration using Hostinger and TLS certificates issued by Let's Encrypt or ZeroSSL.

Artifact	River of Phish	COLDRIVER
Domain Registrars	Namecheap, Hostinger	Namecheap, Hostinger, others

Artifact	River of Phish	COLDRIVER
TLS Certificate Issuers	ZeroSSL, Let's Encrypt	ZeroSSL, Let's Encrypt, others

Table 6: Comparing River of Phish and COLDRIVER domain registrars and TLS issuers.

In addition, reporting shared by PwC detailed recent COLDRIVER activity and validated our attribution of both PDFs and domains from this campaign.

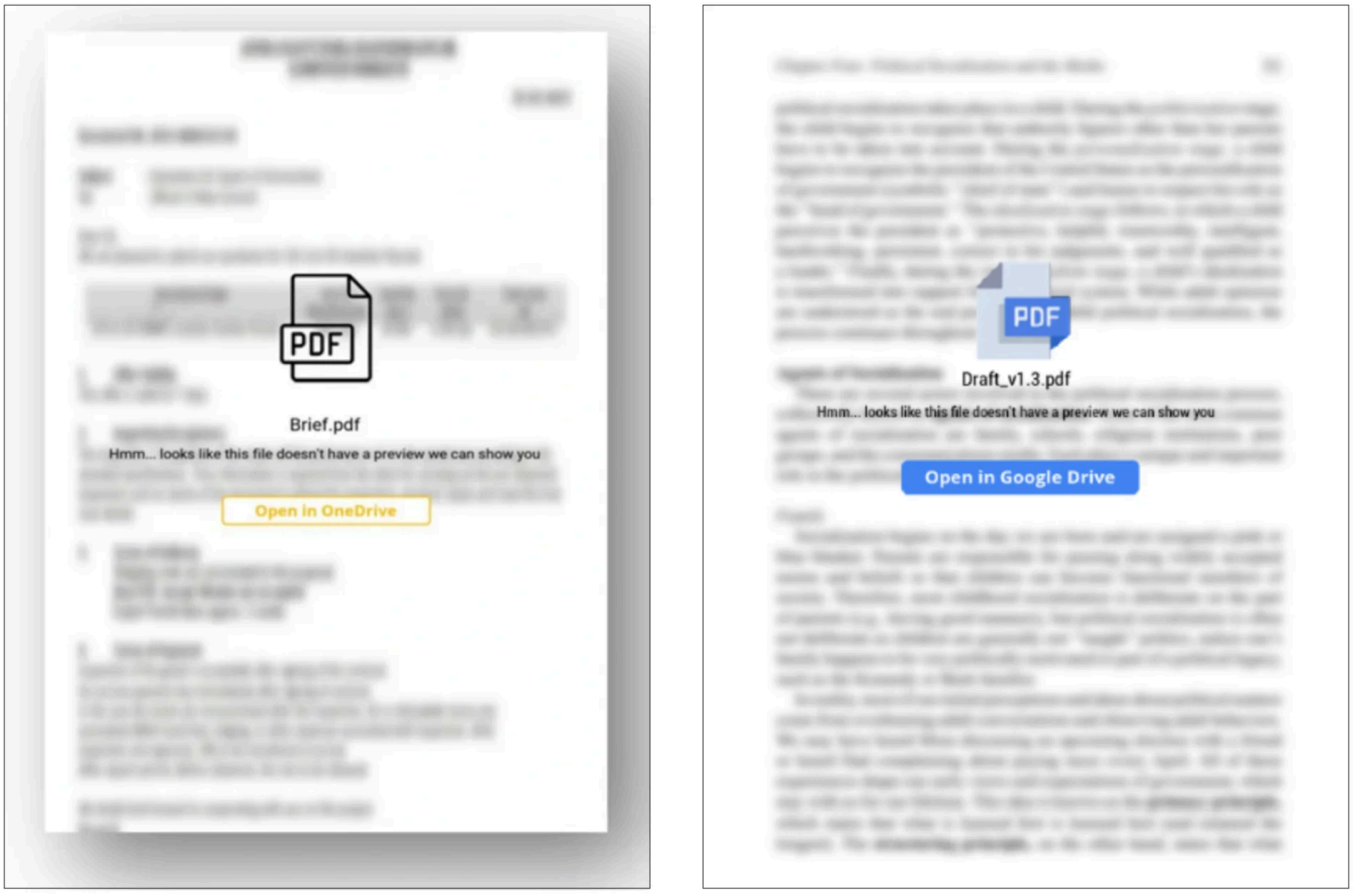
Additional TTP Overlap with Prior Public Reporting on COLDRIVER

Additionally, we noted that River of Phish employed a number of known TTPs of COLDRIVER.

The social engineering and spear-phishing delivery methodology remained consistent across past COLDRIVER activity and the current campaign we are tracking. These methods include:

- Impersonating a known individual by setting up a Proton Mail account using their name;
- Using information gained through reconnaissance to tailor the message in the initial email to make it look more authentic;
- Employing language indicating a desire to collaborate on a shared area of interest; and
- Using a fake password protected/encrypted PDF with the content blurred in the preview.

In one case, a RoP PDF features the text "*Hmm… looks like this file doesn't have a preview we can show you*" (an error message shown by multiple Microsoft services when a file is not previewable) and a 2023 PDF from COLDRIVER features the identical text (Figure 4).



(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2024/08/stitched-figure10.png&nocache=1)

Figure 4: PDF sent in a campaign reported by Microsoft in December 2023 (https://www.microsoft.com/en-us/security/blog/2023/12/07/star-blizzard-increases-sophistication-and-evasion-in-ongoing-attacks/) (left); PDF from the River of Phish campaign (right).

Finally, a PDF sent to one of the targets we examined contains multiple RoP elements, as well as an additional element previously associated with COLDRIVER. Specifically, the PDF contained an embedded link using a Customer Relationship Management (CRM) service previously reported as used by COLDRIVER, not a direct link to actor-registered infrastructure. In almost all other aspects, the document matched the RoP campaign. The PDF was sent in March 2024 and named "RS_version 1.3.pdf". The email sender masqueraded as a retired US official seeking comment on a report on Ukraine. Language in the email describing a purported report and requesting a review was identical to other RoP emails. The attached PDF matched all RoP metadata, and the name used variants on "RS" and "Draft 1.3" naming observed in multiple RoP PDFs (See: *Figure 2*). However, unlike the other PDFs that included a direct link to a first-stage domain, this file included a link through HubSpot, a CRM provider.

```
dj-kqf04.eu1.hubspotlinksfree[.]com/Ctc…
```

In 2023 Microsoft identified COLDRIVER as a HubSpot user, and specifically noted (https://www.microsoft.com/en-us/security/blog/2023/12/07/star-blizzard-increases-sophistication-and-evasion-in-ongoing-attacks/) the practice of embedding HubSpot domains in the targeting PDF in an attempt to evade detection.

River of Phish: Signs of Continued Evolution?

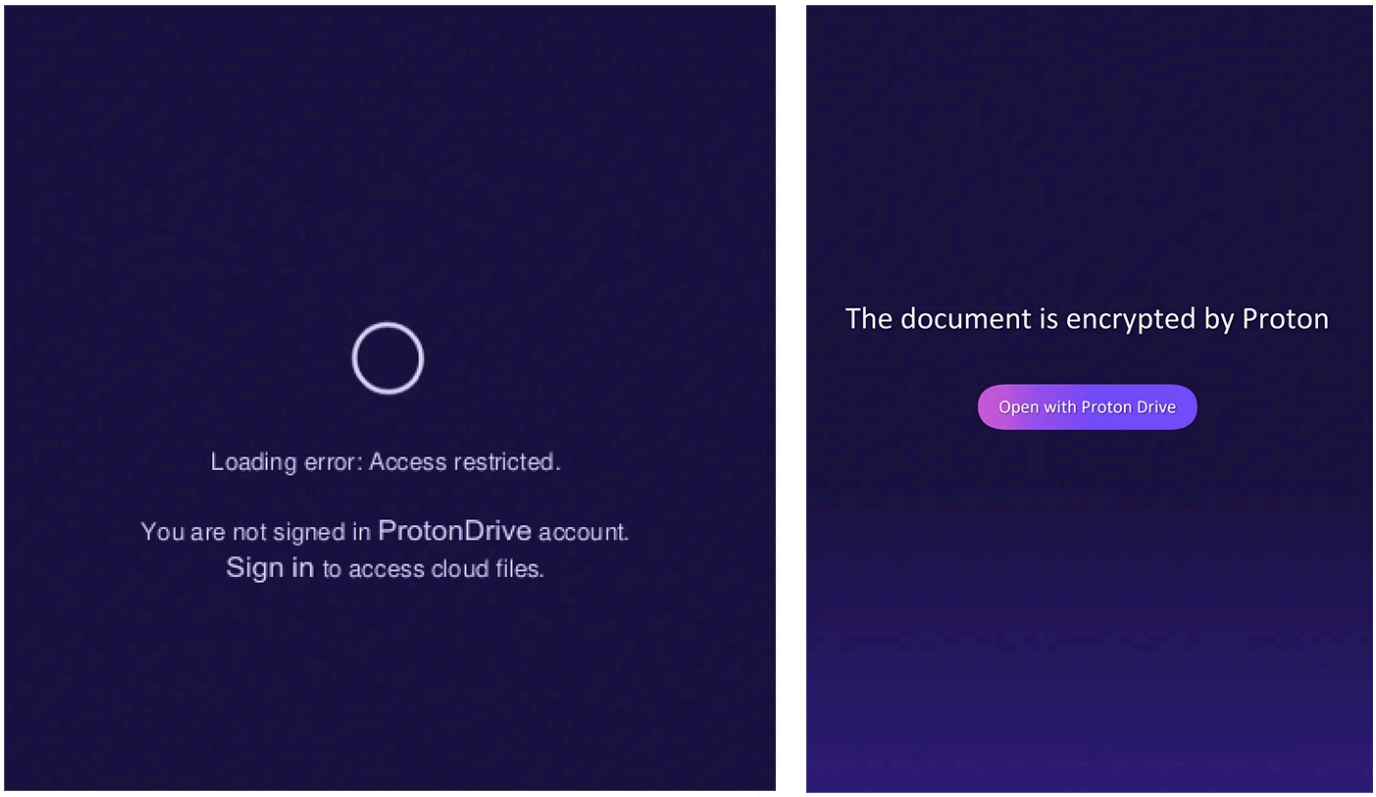
In addition to the previous use of HubSpot, earlier COLDRIVER reporting mentioned clusters of domains named around a particular theme or service being impersonated, such as *proton-docs[.]com*, *proton-reader[.]com*, and *proton-viewer[.]com* reported by Microsoft in 2022 (https://www.microsoft.com/en-us/security/blog/2022/08/15/disrupting-seaborgiums-ongoing-phishing-operations/). However both Microsoft (https://www.microsoft.com/en-us/security/blog/2023/12/07/star-blizzard-increases-sophistication-and-evasion-in-ongoing-attacks/) and Recorded Future (https://www.recordedfuture.com/research/bluecharlie-previously-tracked-as-tag-53-continues-to-deploy-new-infrastructure-in-2023) noted that COLDRIVER appeared to be using a "more randomized (https://www.microsoft.com/en-us/security/blog/2023/12/07/star-blizzard-increases-sophistication-and-evasion-in-ongoing-attacks/)" domain generation mechanism starting in 2023, suggesting adaptation to previous detection techniques, and an effort to hide targets. RoP first-stage infrastructure did not include any themes in domain naming, however we note that our report focuses specifically on civil society clusters and thus it is possible that COLDRIVER is using other domain naming schemas against other targets.

Previous reporting also identified COLDRIVER domains registered through Namecheap. During this campaign we observed that the domain registrar of choice changed to Hostinger sometime between January and March of 2024. PwC reporting (https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/blue-callisto-orbits-around-us.html#footnotes) highlighted that COLDRIVER has previously used Hostinger as a registrar in 2022, however more evidence is needed to determine whether this is a change that will persist across future COLDRIVER activity.

In addition to the analysis in this section, we have also developed a YARA rule (See: Appendix) that will assist other researchers in identifying other PDF files likely attributable to River of Phish / COLDRIVER.

4. COLDWASTREL: A New Threat Actor Surfaces?

In March 2023, our investigative partner Access Now began receiving cases of personalized phishing. The first were shared by the Russian human rights organization First Department. Access Now shared the cases with The Citizen Lab. Superficially, the messages had much in common with COLDRIVER. For example, the attacker sent PDF attachments with references to ProtonMail and ProtonDrive designed to trick targets into clicking on a link. However, close analysis revealed numerous differences, ultimately leading us to conclude that these were the work of a separate threat actor.



(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2024/08/stitched-figure11.png&nocache=1)

Figure 5: Screenshots from COLDWASTREL PDFs.

Consistent Differences Between Bait PDFs

This campaign deviates in several important aspects from COLDRIVER, such as the characteristics of the malicious PDF (*see Table 7*) and front-end infrastructure. At this time, we assess that this activity cluster is not the work of the COLDRIVER operator and warrants further investigation.

	COLDRIVER	**COLDWASTREL**
PDF Version	1.4	1.5
PDF Language	en-US	ru-RU
PDF Author	Plausible-yet-obscure English language names	“User”
Links in PDF	Unique to each PDF	Consistent across mu
Links in PDF	Redirected to fingerprint, then to separate domain/site to gather credentials	Hosted the phishing

Table 7: Overview of differences in the PDFs and infrastructure between two campaigns that shared similarities in social engineering and credential harvesting.

Our colleagues at Access Now have identified an additional COLDWASTREL PDF on VirusTotal which we include here to assist other researchers in pursuing this threat actor.

COLDWASTREL PDF on VirusTotal

```
4a9a2c2926b7b8e388984d38cb9e259fb4060cccc2d291c7910be030ae5301a3
```

Infrastructure Differences

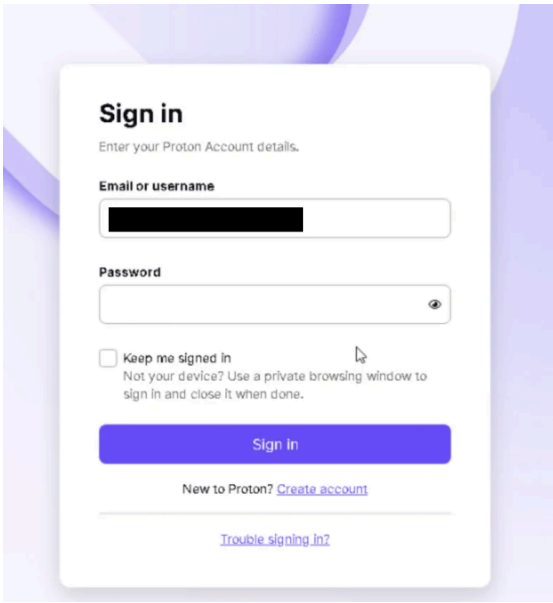
In addition to the differences in the PDF content and metadata, there were several other notable differences between the two attacks:

- All pre-2024 COLDWASTREL PDFs contained a link to the same domain, *protondrive[.]online*. This tactic deviates from the COLDRIVER activity that we investigated, which seemed to use a different domain for each PDF, without making use of a lookalike domain.
- The domain *protondrive[.]online* also differs from the infrastructure seen with COLDRIVER. The domain was registered through URL Solutions Inc, which deviates from the RoP/COLDRIVER TTPs described above.

Together with Access Now, we are referring to this operator as COLDWASTREL. We hope that other research teams will be able to advance this investigation further using indicators provided in Access Now's report (https://www.accessnow.org/publication/russian-phishing-campaigns/). While we are not attributing this campaign, and have only a limited number of targets, we note that the COLDWASTREL targeting that we have observed does appear to align with the interests of the Russian government.

Fresh COLDWASTREL?

Shortly prior to publication of this report, we have tentatively identified what appears to be renewed COLDWASTREL targeting, based on TTPs, targeting overlap and infrastructure similarity. In this attack, the decoy PDF included the domain *protondrive[.]me* which, when clicked, redirected to phishing hosted at *protondrive[.]services*.



(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2024/08/image1-1.png&nocache=1)

Figure 6: An August 2024 COLDWASTREL phishing page. The prepopulated email address of the target has been redacted.

5. Why Do Some Governments Still Phish?

Governmental threat actors, including in states that possess a high degree of technical competency (e.g. reserves of zero-day exploits), continue to phish *because personalized phishing still works*. When the cost of discovery remains low, phishing remains not only an effective technique, but a way to continue global targeting while avoiding exposing more sophisticated (and expensive) capabilities to discovery.

Threat actors like the FSB are equipped with substantial intelligence gathering and analytical capabilities. They possess a detailed window into potential targets' relationships and work activities which enables operators to craft very credible phishing lures. Research shows that phishing leveraging personal information has a much higher probability of success (https://www.sciencedirect.com/science/article/abs/pii/S0003687022002319), and we speculate that a mature phishing campaign against a longstanding target benefits from a positive feedback loop in which more cycles of phishing yield ever-more detailed information that can be used to create increasingly convincing lures for future victims.

Where we do see evolution and tactical cleverness from COLDRIVER, it remains just enough to bypass certain modes of discovery. For example, in the River of Phish campaign, we see a wide range of paired sender names, domains, and PDF metadata. It is possible that these pairings are each used for only a very small number of targets. This approach may indicate efforts to evade detection by popular email platforms.

As platform and endpoint security continues to thwart attacks, attackers must rely on increasingly sophisticated social engineering that can be hard to distinguish from normal communications. Confirming the authenticity of the message and sender will protect both parties, and is well worth the extra time and effort. As COLDRIVER's operators must know, this is not a practical action for every message.

Smash & Grab Phishing?

Numerous features of COLDRIVER's activities increase the chance of a successful compromise while also increasing the chance that a sophisticated target or analyst will identify the communications as malicious.

For example, impersonating an individual known to the target increases the likelihood of discovery because the target can usually contact the impersonated individual to inquire whether the communication is authentic. This chance of discovery is compounded by the use of a bait document ruse that is also likely to lead to puzzled victims, reports, and eventual discovery.

This sort of social engineering tactic is well suited to a persistent adversary that does not face reputational or criminal penalties from discovery. For example, the operators of COLDRIVER presumably enjoy the protection of the Russian government, and know better than to schedule a holiday at Disney World in Florida.

While the volume of past reporting on COLDRIVER has probably disrupted specific campaigns, it is unlikely to put a stop to their activity. Indeed, we see evidence that the operator makes minimal changes in their tactics in response to disruptions. Such changes buy them a modest window of time to continue targeting even though a degree of discovery, including further exposure by researchers and even governments, remains inevitable.

6. The Russian Cyber Espionage Landscape

Russia has a long history (https://us.macmillan.com/books/9780374287269/activemeasures) of espionage that reaches back to pre-Soviet times, and has engaged in cyber espionage campaigns and active cyber operations for decades (https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/). These operations have been extensively studied by academics (https://direct.mit.edu/isec/article/46/2/51/107693/The-Subversive-Trilemma-Why-Cyber-Operations-Fall), civil society (https://carnegieendowment.org/research/2024/02/russias-countervalue-cyber-approach-utility-or-futility?lang=en) organizations, journalists (https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/), governments (https://www.cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf) and the commercial (https://www.microsoft.com/en-us/security/blog/2023/12/07/star-blizzard-increases-sophistication-and-evasion-in-ongoing-attacks/) cybersecurity (https://cloud.google.com/blog/topics/threat-intelligence/apt44-unearthing-sandworm) community. Generally, Russian cyber espionage and active cyber operations are undertaken independently by multiple (and sometimes competing (https://ecfr.eu/archive/page/-/ECFR_169_-_PUTINS_HYDRA_INSIDE_THE_RUSSIAN_INTELLIGENCE_SERVICES_1513.pdf)) state security agencies, occasionally with the participation of organized criminal groups (https://www.nytimes.com/2017/03/12/world/europe/russia-hacker-evgeniy-bogachev.html) or other private sector entities (e.g., NTC Vulkan (https://www.washingtonpost.com/national-security/2023/03/30/russian-cyberwarfare-documents-vulkan-files/), RomCom (https://www.microsoft.com/en-us/security/blog/2023/07/11/storm-0978-attacks-reveal-financial-and-espionage-motives/), Cadet Blizzard (https://www.microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/)).

There are several Russian and Russian-aligned entities that undertake or are responsible for cyber espionage (see here (https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet#cyber-operations-and-the-russian-intelligence-services)). Russia's foreign intelligence service, the SVR (*Sluzhba Vneshney Razvedki*), is responsible for foreign intelligence gathering and is generally known for long-term espionage campaigns such as those publicly referred to as APT29, "Cozy Bear" or "The Dukes." SVR-linked campaigns have typically involved (https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-057a) accessing credentials of targeted entities through password spraying, brute forcing, and other means of accessing cloud and other accounts.

Russia's main intelligence directorate of the armed forces, the GRU, is associated with cyber espionage and cyberwarfare (https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary#letter-c) operations designated as APT28, Fancy Bear, and Sandworm, and has been linked to DDoS (https://www.gov.uk/government/news/uk-assess-russian-involvement-in-cyber-attacks-on-ukraine) and disruptive malware (https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and) attacks (https://www.penguinrandomhouse.com/books/597684/sandworm-by-andy-green-

berg/) on critical infrastructure, the financial sector, government and non-governmental organizations, and other sectors. The US, UK and other Western governments have also linked (https://media.defense.gov/2024/Feb/27/2003400753/-1/-1/0/CSA-Russian-Actors-Use-Routers-Facilitate-Cyber_Operations.PDF) this entity to the compromise of edge routers in order "to host spear-phishing landing pages and custom tools."

Meanwhile, Russia's FSB has responsibilities covering internal security, counterintelligence, and foreign espionage. Two units within the FSB, Centre 16 and Centre 18, are responsible for cyber espionage, with the activities of COLDRIVER falling under the umbrella of the latter. According to a UK government assessment (https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet#cyber-operations-and-the-russian-intelligence-services), Centre 18 is also known as the Centre for Information Security (TsIB) Military Unit 64829.

7. Civil Society Targeting by Russia: Always Present

Cyber espionage campaigns and active cyber operations targeting government entities, critical infrastructure, businesses and financial institutions have traditionally received the bulk of commercial cybersecurity firms' and media attention. However, this selection bias (https://www.tandfonline.com/doi/full/10.1080/19331681.2020.1776658) arising from commercial priorities has produced a distorted view of the overall victim set. Until recently, attacks targeting civil society tended to be overlooked in industry and government reporting because civil society lacks the resources to pay for high-end services, which means that indicators that might be gleaned from civil society may be largely unseen by cybersecurity firms.

A major takeaway (https://targetedthreats.net/) of the last decade and a half of The Citizen Lab's research into digital espionage is that civil society is a major and often overlooked (https://circleid.com/posts/20130304_-civil_society_hung_out_to_dry_in_global_cyber_espionage/) segment, despite being targeted by the same groups that attack government and industry. Authoritarian governments are particularly sensitive to political opposition, dissidents and investigative journalism and routinely orient (https://www.foreignaffairs.com/world/autocrat-in-your-iphone-mercenary-spyware-ronald-deibert) their cyber espionage campaigns towards groups involved in those activities, both at home and abroad. Cyber espionage against civil society is also a major component of digital transnational repression (https://citizenlab.ca/2022/03/digital-transnational-repression-explained/), which has been growing in scope and scale worldwide.

In 2017, for example, The Citizen Lab published a report (https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/) detailing a Russia-aligned hack and leak operation, which we called "Tainted Leaks." The investigation detailed an extensive phishing operation targeting 200 unique individuals across 39 countries. Those targets included senior government and military officials, CEOs of energy companies, and civil society. We discovered that civil society targets, including academics, journalists, activists, and members of NGOs, represented the second largest cluster set (21%), after government officials. Although we could not attribute that operation to a single entity, there were several indicators suggesting links to APT28, a Russian threat actor affiliated with the GRU.

These cyber attacks targeting civil society are gaining wider visibility, thanks in part to the 10 plus years of reporting by The Citizen Lab, Access Now, Amnesty International, investigative journalists, and media consortia. The US, UK, Canada and other Western governments, as well as cybersecurity (https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023) firms (https://radar.cloudflare.com/reports/project-galileo-9th-anniv), have formally (https://www.cisa.gov/news-events/alerts/2024/05/14/cisa-and-partners-release-guidance-civil-society-organizations-mitigating-cyber-threats-limited) acknowledged (https://www.canada.ca/en/communications-security/news/2024/05/canada-joins-international-security-partners-in-release-of-advisory-guidance-on-growing-cyber-security-threat-to-civil-society.html) the frequency of and risks to civil society stemming from cyber espionage and cyber operations, now echoing civil society's reporting.

Other Digital Threats to Civil Society Groups Working On and In Russia

Civil society is under extreme threat in Russia. A recent study (https://jfj.fund/attacks-on-media-workers-in-russia-in-2021-2023/) conducted by the Justice for Journalists Foundation counts a total of 5,262 cases of attacks/threats against professional and civilian media workers and editorial offices of traditional and online media, as well as against Russian journalists abroad in 2021-2023.

For those still residing inside the country, the threat of raids and seizure of equipment is ever-present. Russia is currently among the top five countries (https://mmdc.ru/blog/2023/12/14/rossiya-okazalas-na-chetvertom-meste-po-kolichestvu-zhurnalistov-za-reshetkoj/) in the world for arrests of journalists. In addition, the threat of physical violence for those located both inside and outside Russia is constant, with journalists and civil society figures regularly beaten (https://novayagazeta.eu/articles/2023/07/04/novaya-gazeta-reporter-elena-milashina-and-attorney-alexander-nemov-attacked-in-russias-chechnya-en-news), tortured (https://www.amnesty.org/en/latest/news/2022/09/russia-activist-allegedly-beaten-and-raped-for-reciting-anti-war-poem-online/), poisoned (https://meduza.io/en/feature/2023/08/15/the-most-likely-explanation), and imprisoned (https://www.cnn.com/2024/03/29/media/russia-journalists-arrested-evan-gershkovich/index.html). Prominent opposition voices (https://meduza.io/en/news/2024/02/16/russian-opposition-politician-alexey-navalny-has-died) have been killed, or have died in custody. Russia is known for its "highly aggressive (https://freedomhouse.org/report/transnational-repression/russia)" practice of transnational repression, which involves the targeting of dissidents, human rights defenders, and other civil society members living in exile/outside Russia through different methods including poisonings and killings.

Beyond these physical threats, civil society groups operating inside Russia, in exile, or other groups working on Russian issues face a wide range of digital threats. A large number of civil society groups and independent media organizations have moved into exile since the 2022 full-scale invasion of Ukraine by Russia (https://books.openedition.org/pressesmines/9128). Today, many organizations-in-exile operate in a geographically dispersed and decentralized manner, making them dependent on online communications. The critical dependence on technology combined with frequent resource constraints makes these groups exceptionally vulnerable to a wide range of digital threats.

Censorship

Communications and information in Russia are subject to an extensive censorship regime, impacting the ability of audiences within Russia to access information and blocking the flow of information out of Russia. These restrictions include direct censorship of websites (https://meduza.io/en/news/2023/09/07/russian-authorities-reportedly-blocked-more-than-885-000-websites-in-first-half-of-2023) and social media platforms (https://www.themoscowtimes.com/2023/07/07/russia-blocks-metas-twitter-competitor-app-lawmaker-a81773) and blocking on specific communications protocols such as VPNs (https://roskomsvoboda.org/ru/analysis/vpn-russia-2023-eng/). This blocking also hampers organizing and coordination between domestic and foreign civil society organizations. For example, a 2023 report (https://citizenlab.ca/2023/07/an-analysis-of-in-platform-censorship-on-russias-vkontakte/) from The Citizen Lab on the Russian social networking site VK discovered that the platform "blocked content posted by independent news organizations, as well as content related to Ukrainian and Belarusian issues, protests, and lesbian, gay, bisexual, transgender, intersex, and queer (LGBTIQ) content."

Threats & Harassment

Prominent critics of the regime, antiwar activists, and independent media regularly face extensive intimidation and harassment campaigns both in and outside of Russia. These campaigns may include highly targeted online threats (https://storage.googleapis.com/istories/stories/2023/09/19/pust-ne-spyat-spokoino-vashi-gnidi/index.html), backed by meticulous research into the personal details and surveillance of the target.

Indirect Censorship Through Malicious Reporting and Pressuring Tech Platforms

Prominent regime targets are often subjected to extensive and coordinated campaigns to report social media accounts and posts on platforms, like Instagram and Facebook, with the goal of triggering account suspensions and post deletions. For example, a prominent Russian researcher and antiwar activist who spoke with us counted 83 complaints against her Instagram account submitted in a single 11-hour period in July 2024. The Russian government has also reportedly applied pressure on companies like Apple and Google to delete opposition (https://www.washingtonpost.com/business/2021/09/17/navalny-google-apple-app-russia/) and VPN (https://www.reuters.com/technology/russia-says-apple-blocks-25-vpn-apps-russia-ifx-reports-2024-07-04/) apps, as well as civil society YouTube videos (https://www.accessnow.org/press-release/youtube-russia-stop-suppressing-free-speech/).

Account Takeovers and Honeypots

Beyond the sophisticated social engineering described in this report, popular chat programs, such as Telegram, are regularly targeted with a range of tactics (https://www.wired.com/story/the-kremlin-has-entered-the-chat/) for account hijacking and takeovers.

The number of tactics to target accounts and private information are too numerous to list, and are constantly evolving. For example, the co-founder of a Russian NGO that assists imprisoned antiwar activists described to us a new attack technique which relies on a fake Telegram "Helpline bot" impersonating the project of a genuine non-governmental organization. Such a fake helpline could be easily used to gather account information and identifying details from at-risk activists inside Russia, potentially as a precursor to eliciting sensitive information or account takeovers.

8. Protect Yourself & Your Colleagues

We believe that COLDRIVER and other Russian-government backed threat actors will persist in targeting civil society. While large email platforms continue to track and seek to disrupt these operators, this case shows that attacks can still make it through their defenses and into inboxes.

Do you think **you have been targeted by COLDRIVER, COLDWASTREL or other kinds of personalized phishing?** We encourage you to contact Access Now's Digital Security Helpline (https://www.accessnow.org/help/) to seek assistance.

Do you think that COLDRIVER or similar governmental phishing groups **may target you in the future**? If so, we encourage you to review the steps below. However, these recommendations are not comprehensive, and there is **no substitute for seeking expert assistance** from competent professionals such as Access Now's Helpline.

The following recommendations have been prepared jointly by Access Now and The Citizen Lab:

Start with prevention

Use two-factor authentication, correctly: Experts agree that setting up two-factor authentication (2FA) is one of the most powerful ways to protect your account from getting hacked.

However, hackers like COLDRIVER and COLDWASTREL may try to trick you into entering your second factor; we have seen attackers successfully compromise a victim who had enabled 2FA. People using SMS-messaging as their second factor are also at greater risk of having their codes stolen, if a bad actor takes over their phone account.

We recommend that people use more advanced 2FA options such as security keys or, if they are Gmail users, Google Passkeys. Here are three guides for increasing the level of security for your account:

- Get Google Passkeys (https://www.google.com/account/about/passkeys/) (Google)
- How to: Enable two-factor authenticatio (https://ssd.eff.org/module/how-enable-two-factor-authentication)n (Electronic Frontier Foundation)
- Set up multi factor authentication (https://securityplanner.consumerreports.org/tool/set-up-multifactor-authentication-mfa) (Consumer Reports)
- Use a security key (https://securityplanner.consumerreports.org/tool/use-a-security-key-for-strongest-mfa) (Consumer Reports)

Enroll in programs for high-risk users. Google and some other providers offer optional programs for people who, because of who they are or what they do, may face additional digital risks. These programs not only increase the security of your account, but also flag to companies that you may face more sophisticated attacks. Such programs include:

- Google Advanced Protection (https://landing.google.com/advancedprotection/)
- Microsoft Account Guard (https://accountguard.microsoft.com)

- Proton Sentinel (https://proton.me/support/proton-sentinel)

Received a message? Be a five second detective

- **Step one: check your inbox for the sender's email.** Ask yourself if you have received messages from this account before. COLDRIVER often uses lookalike emails to impersonate people known to the target either personally or professionally, so may see an email that appears to come from someone you know, writing about something you would expect them to write about. Even if you have received previous messages from the same email address, it is possible to "spoof" a familiar looking email address, so move on to the next step.

- **Step two: check with the sender over a different medium**. If you have any concerns or are at all suspicious, do not open any PDF attachment or click on any link sent in the email. Instead, check directly with the purported sender, via another service, to confirm whether or not they've reached out to you. If you don't already have direct contact with them, consider asking someone you trust to inquire on your behalf.

- **Step three: don't just click.** Always consult an expert before opening a document you are unsure about. If you want to view a document that you think is probably safe, but want to take care, open the file *within* your webmail. Google, Microsoft, and others open the files on their computers and display the contents to you. This protects you from malicious code embedded in a document. But it **will not prevent you from clicking on potentially malicious links inside the document.**

    - If you are viewing an attached document inside your webmail, you should remain careful. **Don't just click on any links**; copy and paste them into your browser before visiting. Examine the domain carefully: Is it what you would expect for the site you expect to be visiting? Advanced phishing kits are very good at impersonating popular services, and often the only visual clue that it is not the authentic site will be in the address bar of the browser.

    - If you see a "login page" pop up, **stop**. This is a good time to consult a trusted expert.

- **Step four: beware of "encrypted" or "protected" PDFs.** This kind of message is almost always a cause for concern. Legitimately encrypted PDFs almost never include a single "click here" button inside the PDF, and they don't show a blurred version of the contents. Never click on any "login" links or "buttons" inside a PDF you have been sent.

Considering Online Virus Checking Sites? You may wish to use online virus scanning sites such as VirusTotal (https://www.virustotal.com/) or Hybrid Analysis (https://www.hybrid-analysis.com/) to check suspicious links or files.

- These services offer a useful service and can be part of a good security practice, but they come with a very important caveat: **when you use such free services, you are not the customer, you are the product.** Your files are available to many researchers, companies, and governments.

- We do not recommend using such tools to check "sensitive" files that may contain personal information or other private topics. Instead, contact a trusted expert that can help.

Think you are being targeted?

These recommendations address the kind of phishing that COLDRIVER and COLDWASTREL are currently using, but there are many other ways you could be targeted Whatever your level of risk, we encourage you to get personalized security recommendations from the Security Planner (https://securityplanner.consumerreports.org/), which also maintains a list of emergency resources (https://securityplanner.consumerreports.org/tool/emergency-resources/) and advanced security guides (https://securityplanner.consumerreports.org/tool/more-anonymity-security-help).

If you suspect that you have already been targeted in an attack, reach out to a trusted practitioner for advice. It is crucial to evaluate any damage to your organization and/or to other related organizations and individuals, such as partners, participants, grantees, and others. If this is the case, keep them informed about what has happened, what has been leaked, how this may impact them, and what steps you are taking to mitigate this impact.

If you believe you have been compromised: Access Now's Digital Security Helpline (https://www.accessnow.org/help/) is available to support members of civil society, including activists, media organizations, journalists, and human rights defenders, 24/7 in nine languages, including Russian (https://www.accessnow.org/help-ru/?ignorelocale).

- **Change your password right away**. If you are using the same password for other accounts, you should change the password for those accounts, too. Consider using a password manager (https://securityplanner.consumerreports.org/tool/get-a-password-manager) to keep track of multiple passwords.
- You can also review access logs on your accounts, such as Proton Mail's Authentication Logs (https://proton.me/support/authentication-logs), Gmail's Last Account Activity (https://support.google.com/mail/answer/45938?hl=en), and review devices with account access (https://support.google.com/accounts/answer/3067630?hl=en), as well as Microsoft's Check recent sign-in activity (https://support.microsoft.com/en-us/account-billing/check-the-recent-sign-in-activity-for-your-microsoft-account-5b3cfb8e-70b3-2bd6-9a56-a50177863357). Some users may still have questions after reviewing these logs. We encourage you to make a copy of the logs if you suspect you may have been targeted, to share with an expert for review.

Acknowledgments

The Citizen Lab would like to express our deepest gratitude to the many targets and organizations with suspect messages that consented to share indicators and materials with us, and discuss their experiences. Without their participation, this investigation would have been impossible.

We would also like to thank many researchers and threat intelligence teams for feedback, including the teams at Mandiant, Microsoft Threat Intelligence Center, Proofpoint, and PwC.

We also thank Friendly Robot and TNG.

Thanks to our colleagues at The Citizen Lab Siena Anstis, Jakub Dalek, Bill Marczak, and Adam Senft for their careful review and editorial assistance, Mari Zhou for graphical assistance and report art, and Snigdha Basu and Alyson Bruce for communications support.

Appendix: Indicators of Compromise

COLDRIVER PDF Hashes

```
b07d54a178726ffb9f2d5a38e64116cbdc361a1a0248fb89300275986dc5b69d
0ded441749c5391234a59d712c9d8375955ebd3d4d5848837b8211c6b27a4e88
efa2fd8f8808164d6986aedd6c8b45bb83edd70ca4e80d7ff563a3fbc05eab89
c1fa7cd73a14946fc760a54ebd0c853fab24a080cbf6b8460a949f28801e16fc
603221a64f2843674ad968970365f182c228b7219b32ab3777c265804ef67b0a
df9d77f3e608c92ef899e5acd1d65d87ce2fdb9aab63bbf58e63e6fd6c768ac3
384d3027d92c13da55ceef9a375e8887d908fd54013f49167946e1791730ba22
79f93e57ad6be28aae62d14135140289f09f86d3a093551bd234adc0021bb827
00664f72386b256d74176aacbe6d1d6f6dd515dd4b2fcb955f5e0f6f92fa078e
```

Yara Rule for River of Phish PDFs

```
rule River_of_phish
{
meta:
   description = "Detects PDFs from COLDRIVER River of Phish Campaign"
   author = "The Citizen Lab"
   date = "2024-08-02"
   version = "1.0"
strings:
   $pdf_header = "%PDF-1.4"
   $producer = /\/Producer\s*\(LibreOffice\\0407\\0560\)/
   $language = /\/Language\s*\(en\\055US\)/
   $uri_pattern =
/https\\072\\057\\057[a-zA-Z0-9]+\\056[a-zA-Z0-9]+\\057[a-zA-Z0-9_]+/nocase


condition:
   $pdf_header at 0 and
   $producer and
   $language and
   $uri_pattern in (0..1500)

}
```


(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2024/08/Yara-rule-for-river-phish-1.png&nocache=1)

COLDRIVER First-stage Domains

ithostprotocol[.]com
xsltweemat[.]org
egenre[.]net
esestacey[.]net
ideaspire[.]net
eilatocare[.]com
vocabpaper[.]com
matalangit[.]org
togochecklist[.]com

COLDWASTREL PDF on VirusTotal

4a9a2c2926b7b8e388984d38cb9e259fb4060cccc2d291c7910be030ae5301a3

COLDWASTREL Domains

protondrive[.]online
protondrive[.]services (tentative)
protondrive[.]me (tentative)
service-proton[.]me (Per Access Now’s analysis)

Privacy Policy (https://citizenlab.ca/privacy/)

Unless otherwise noted this site and its contents are licensed under a Creative Commons Attribution 2.5 Canada (https://creativecommons.org/licenses/by/2.5/ca/) license.

munkschool OF GLOBAL AFFAIRS & PUBLIC POLICY UNIVERSITY OF TORONTO

(http://munkschool.utoronto.ca/)

Phishing Attacks Targeting Ukrainian NGOs for AccessNow

For 7 years, Digital Security Lab Ukraine has been providing security support to the civil society sector in Ukraine. Thanks to our long-standing work, we have had the opportunity to observe changes in this field, document security incidents, and conduct risk assessments together with our beneficiaries and partners.

Among the common risks, our beneficiaries rate account hacking as the highest risk. They consider device compromise to be significantly less likely. However, it's important to note that risk assessment largely depends on the organization's activities, its products or results, and the broader context. When detailing the risks, we see that the greatest concern is caused by phishing-based account compromises and device compromise through the installation of malicious software.

From our side, as we document security events (incidents), we observe regular waves of targeted phishing campaigns and consistently high levels of mass commercial phishing.

Regarding the assets most frequently targeted by phishing attacks, these are services commonly used by representatives of the Ukrainian civil society sector. Among the most popular are Google, Microsoft, Ukr.net, Facebook, Instagram, Telegram, X (Twitter), WhatsApp, and Signal. The largest share of successful phishing attacks targets online accounts, where attackers impersonate legitimate customer support representatives. In particular, since 2022, due to Ukrainians actively highlighting the consequences of Russian aggression, social media platforms have increased often unjustified content or account blockings (Facebook, Instagram). This trend is exploited by attackers in their phishing campaigns, impersonating platform support teams and threatening to block accounts. You can find examples of such campaigns at this or this link.

Similar tactics are used by attackers in phishing through popular messengers. From 2022 to 2024, we've seen the highest number of such cases in Telegram. Attackers impersonate Telegram support, intimidate users by claiming that someone has gained access to their account, and ask them to verify their account ownership. This way, they obtain the SMS code, two-factor authentication password, or prompt users to add a new session. Another common scheme involves using bots that imitate official sources of information about current events, such as power outages. In the case of Telegram, the situation is further complicated by the company's lack of communication with users and failure to respond to malicious activities.

There is growing concern about phishing in messengers and services that are positioned as "secure" (using end-to-end encryption). In Proton, Signal, and WhatsApp, attackers exploit several beliefs at once. First, the idea that people tend to trust more in "secure" services and may react less cautiously to phishing messages. Second, the use of political context. In Ukraine, petition services are a popular way of influencing the government, so attackers create phishing

messages and websites exploiting these services. We've described this scheme in more detail in this publication.

In account hacking attempts, it is often difficult for us to attribute the attack due to a lack of technical, human, financial, or other resources, or the inability to gather indicators. However, in the case of phishing attacks with malicious attachments, they contain significantly more indicators. We can obtain the original message, analyze IOCs and TTPs, and compare them with known past incidents or reports. Over the years, we have observed waves of targeted phishing attacks using malicious attachments. These are usually associated with hacker groups sponsored by Russia, and less frequently with financially motivated attacks. Attackers attempt to impersonate official government agencies, such as the Security Service of Ukraine (SBU), courts, tax authorities, military structures, and others.

The most common goal of such phishing is espionage, and less frequently, the destruction or restriction of access to data. In such cases, phishing may serve as the initial stage for more complex tasks (initial access). Malicious software most often targets Windows OS, although there have been cases involving Android OS. Among the actors most often attributed, we have seen Gamaredon (Primitive Bear, Tridentursa), but we do not have enough data for statistical analysis.

Ksenia Maximova | founder/director Russian Democratic Society UK

This breach was deeply troubling for us as an organization. Firstly, the email appeared to be from a founder or director of a prominent US-based organization, making it particularly deceptive. I had shared the file with two other human rights activists, potentially amplifying the breach.

Our Google Suite was down for three days, which severely hindered our ability to assist another NGO with their grant application for the evacuation of LGBTQA+ individuals persecuted in Russia. We lost access to our calendar and missed other critical communications, setting us back significantly from an operational standpoint.

The breach also created a tense atmosphere, adding to the stress our team is already facing as Russian activists are being targeted globally. Some of our activists still travel to Russia, and this incident further heightened their anxiety. Even though we are based in a supposedly "safe" country, this breach made us feel vulnerable and reachable anywhere.

To make matters worse, my name was later used in a phishing attempt targeting another prominent individual, eroding trust in an already fragile environment. We were forced to conduct a comprehensive review of our IT and personal security, which took over two weeks. Given that we have no paid staff, this added an enormous workload, straining the mental and physical health of our activists, who are already working tirelessly.

Our media outlet focuses on exposing social injustices and human rights violations faced by marginalized groups in Russia. Our team of journalists and editors remain in the country to provide truthful reports on the lives of ordinary people in various regions, as well as the negative impact of the war on our society. Following a recent attack, wrongdoers accessed all our financial records, grant applications and reports, and employee contracts. This information has now been leaked to the public, which poses a very serious safety risks for us, as collaborating with foreign organizations is now illegal in Russia. Propaganda channels with large audiences are already urging authorities to imprison our staff and declare our outlet an "undesirable organization." We are threatened with criminal prosecution, confiscation of private property and physical security risks, and our publication is at risk of closure.

I work as a publisher for an independent investigative media outlet Proekt - we are known for hard-hitting investigations about the Russian State, Vladimir Putin and his family, people involved in war crimes etc. (some of our recent investigations led to sanctions by US and EU of particular persons and companies). We were banned in Russia in summer 2021 and since then are working from exile, our team members now live all over the world, including Europe, USA and Central Asia. We are constantly threatened and dealing with hacking attempts from Russian State-linked groups, but this time it was the most elaborate attempt.

In November 2023 I was approached by a person from another media organization through email, the email contained an invitation to participate in their new media platform. The letter contained a file attached, that by clicking would open at the Proton Drive system. I exchanged several letters with this person without opening the file, until I started to notice that it looks like a phishing attempt. I checked the data more closely and eventually discovered that these were hackers that impersonated a person I knew in real life. The file contained a link to the website that looked exactly like the Proton Drive website. At this point I reached out to Citizen Lab / Access Now for assistance, and then they established that the hackers were from STARBLIZZARD/COLDRIVER group, connected to FSB of Russia.

The consequences of a successful attack would extend beyond breaching privacy. It could expose details of our financial operations, communications with other independent Russian organizations in exile, and personal data of our team members worldwide. Additionally, hackers could use a compromised email to impersonate me, reaching out to others and gathering information under false pretenses. This would undoubtedly erode the trust society has in our work.

Polina Machold, Proekt (www.proekt.media)

‘The Ark’ (‘Kovcheg’) project
https://kovcheg.live
team@kovcheg.live

September 03, 2024

‘The Ark’ project was launched in March 2022 as a project to assist Russians who are against the war in Ukraine. Mass arrests of protesters, repressive laws, widespread ‘military censorship’, and mobilisation forced many Russians to leave their country due to security threats. ‘The Ark’ is the largest project that centrally assists Russians fleeing Russia due to anti-war beliefs. In Russia, ‘The Ark’ has been declared a foreign agent by the Russian Ministry of Justice.

With this letter we provide a statement regarding the impact of the STARBLIZZARD/COLDRIVER phishing attacks that targeted me and my organization, "The Ark" (Kovcheg), which supports Russian emigrants and individuals facing political persecution.

Recently, I was the target of a phishing attempt, aimed at compromising my email account. This incident poses a significant threat not only to me personally but also to the vulnerable individuals we assist. "The Ark" works with people who are fleeing Russia due to political persecution, many of whom are at risk of arrest, imprisonment, or worse due to their anti-war stance. These individuals rely on our support for legal, psychological, and humanitarian assistance as they seek safety in countries like Armenia, Georgia, and beyond. We currently provide support to people in 49 countries, and the security of our communications is paramount in ensuring their safety.

If these phishing attempts had been successful, the potential for harm would have been catastrophic. A breach of our communications could expose sensitive information about these individuals, their locations, and the details of their asylum processes. Such a compromise could result in severe repercussions, including the arrest or persecution of these individuals and their families. It would also erode the trust they place in us, damaging our ability to provide support.

Furthermore, the constant threat of cyberattacks from groups like STARBLIZZARD/COLDRIVER adds significant psychological stress to our daily operations. As we assist people who are already under immense pressure due to political threats, maintaining the security of our communication channels is crucial. Every phishing attempt raises fears that our efforts to protect human rights and support those fleeing persecution could be undermined.

Given the scale and importance of the work we do, it is vital that the infrastructure used by STARBLIZZARD/COLDRIVER is dismantled to prevent further harm. These attacks represent a direct threat to civil society and the human rights defenders we serve. I hope this statement helps demonstrate the real-world consequences of allowing such actors to continue their malicious activities.

If you have any additional questions, feel free to contact me.

Sincerely,
Anastasia Burakova
Founder of ‘The Ark’ project
anastasburakova@gmail.com
+995 557 622 531

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Microsoft Corporation, a Washington State Corporation, NGO-ISAC, a New York State Non-Profit Organization, Plaintiffs, v. John Does 1-2, Controlling A Computer Network and Thereby Injuring Plaintiff and Its Customers, Defendants.	Civil Action No. **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5.1**

DECLARATION OF JEFFREY L. POSTON IN SUPPORT OF PLAINTIFFS' *EX PARTE* APPLICATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, Jeffrey L. Poston, hereby declare and state as follows:

1. I am a partner at the law firm of Crowell & Moring LLP ("Crowell"), and counsel of record, for Plaintiffs Microsoft Corporation ("Microsoft") and NGO Information Sharing and Analysis Center ("NGO-ISAC"). I make this declaration in support of Plaintiffs' Application for an Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Application"). I make this declaration of my own personal knowledge and, if called as a witness, I could and would testify competently to the truth of the matters set forth herein.

I. PARTIES

1. Microsoft and NGO-ISAC seek an Emergency *Ex Parte* Temporary Restraining Order And Order To Show Cause Re Preliminary Injunction designed to disrupt the technical infrastructure employed by John Does 1-2 ("Defendants"), Russian-based

cybercriminals. These Defendants engage in elaborate spear phishing[1] campaigns, whereby the Defendants misuse Microsoft's trademarks and good will to access illegally the systems and data of Microsoft's customers, including NGO-ISAC and leverage this illegal access to impersonate individuals and organizations online, infiltrate email accounts, and exfiltrate-or steal- sensitive and confidential information from online accounts. To manage and direct this illegal activity, these Defendants have established and operate a network of websites and domains, which they use to target their victims, compromise their online accounts, compromise the security of their networks, and steal sensitive information from them. This cybercriminal operation is known as "Star Blizzard." The Star Blizzard Defendants' criminal acts cause irreparable harm to Microsoft, its customers, NGO-ISAC, its member organizations, and the public.

2. As counsel of record for Plaintiffs, I am aware of previous efforts brought by Microsoft to disable other types of unlawful, cybercriminal activities, including the "**Waledac**" Botnet in February 2010 in the Eastern District of Virginia, the "**Rustock**" Botnet in March 2011 in the Western District of Washington, the "**Kelihos**" Botnet in September 2011 in the Eastern District of Virginia, the "**Zeus**" Botnets in March 2012 in the Eastern District of New York, the "**Bamital**" Botnet in February 2013 in the Eastern District of Virginia, the "**Citadel**" Botnets in May 2013 in the Western District of North Carolina, the "**ZeroAccess**" Botnet in November 2013 in the Western District of Texas, the "**Shylock**" Botnet in June 2014

[1] Spear phishing, as used by Plaintiffs Microsoft and NGO-ISAC in this action, is a type of personalized attack in which the threat actor or cybercriminal attempts to acquire sensitive information or access a computer by sending a fake email message that appears to be legitimate, with the goal of having the victim interact further with the email (referred to as the "lure"). *See* Declaration of Sean Ensz in Support of Plaintiffs' TRO Application ¶ 5.

in the Eastern District of Virginia, the "**Ramnit**" Botnet in February 2015 in the Eastern District of Virginia, the "**Dorkbot**" Botnet in November 2015 in the Eastern District of New York; the "**Strontium**" threat infrastructure in August 2016 in the Eastern District of Virginia; the "**Phosphorous**" threat infrastructure in March 2019 in the District of Columbia; the "**Thallium"** threat infrastructure in December 2019 in the Eastern District of Virginia; "**Trickbot**" threat infrastructure in October 2020 in the Eastern District of Virginia; the "**ZLoader**" malware operation in April 2022 in the Northern District of Georgia; the "**Bohrium**" threat infrastructure in May 2022 in the Eastern District of Virginia; and the "**Cracked Cobalt Strike**" cybercriminal and malware operation in March 2023 in the Eastern District of New York.

3. Based on my previous experience with similar cybercriminal defendants that conduct their operations using an infrastructure consisting of a set of websites and domains, *ex parte* relief is necessary, as notice to the Star Blizzard Defendants would allow them to destroy the evidence of their illicit activity and give them an opportunity to move the instrumentalities they use to conduct their unlawful activity. This would render the further prosecution of this matter futile.

4. Indeed, in circumstances where similarly situated cybercriminals and threat groups have learned of Microsoft's attempts to disable the cybercriminal operation, they have attempted to migrate that botnet's command and control infrastructure or activate new domains to prevent their technical infrastructure from being taken down and seized. This has happened both when Microsoft previously brought a takedown against Rustock Botnet, Dorkbot Botnet, and ZeroAccess Botnet. Based on my knowledge of prior similar experiences, I conclude that there is a similar risk that the Star Blizzard Defendants here would take similar evasive action

if they were made aware of the attempts to takedown their technical infrastructure before the takedown was complete.

5. Plaintiffs' counsel has not attempted to provide notice of the TRO Application to the Star Blizzard Defendants, and should not be required to provide notice at this time. I respectfully submit that good and sufficient reasons exist for this TRO Application to be made by Order to Show Cause in lieu of by notice of motion. Microsoft has previously sought *ex parte* temporary restraining orders in United States District Courts in *Microsoft Corporation v. John Does 1-27*, Case No. 1:10-cv-00156 (E.D. Va. 2010) (Brinkema, J.); *Microsoft v. John Does, 1-11,* Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.); *Microsoft Corporation v. Dominique Piatti et al.*, Case No. 1:11-cv-01017 (E.D. Va., 2011) (Cacheris, J.); *Microsoft Corporation et al. v. John Does 1-39 et al.*, Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.); *Microsoft Corporation v. Peng Yong et al.,* Case No. 1:12-cv-1005 (E.D. Va. 2012) (Lee, J.); *Microsoft Corp. v. John Does 1-18 et al.*, Case No. 1:13-cv-139 (E.D. Va. 2013) (Brinkema, J.); *Microsoft v. John Does 1-82*, Case No. 3:13-CV-00319 (W.D. N.C. 2013) (Mullen, J.); *Microsoft v. John Does 1-8*, Case No. A-13-CV-1014 (Sparks, J.) (W.D. Tex 2013); *Microsoft v. John Does 1-8,* Case No. 1:14-cv-811 (O'Grady, J.) (E.D. Va. 2014); *Microsoft v. John Does 1-3,* Case No. 1:15-cv-240 (Brinkema, J.) (E.D. Va. 2015); *Microsoft v. John Does 1-5,* 1:15-cv-06565 (E.D.N.Y. 2015); *Microsoft Corporation v. John Does 1-2,* Case No. 1:16-cv-993 (E.D. Va. 2016) (Lee, J.); *Microsoft Corporation v. John Does 1-2*, Case No. 1:19-cv-00716 (D.C. 2019) (Berman-Jackson, J.); *Microsoft Corporation v. John Does 1-2,* Case No. 1:19-cv-01582 (E.D. Va. 2019) (O'Grady, J.); *Microsoft Corporation and FS-ISAC, Inc. v. John Does 1-2,* Case No. 1:20-cv-1171 (E.D. Va. 2020) (Trenga, J.); *Microsoft, FS-ISAC, and Health-ISAC v. Malikov et al.*, Case No. 1:22-cv-1328 (N. D. Ga. 2022) (Cohen,

J.); *Microsoft v. John Does 1-2*, Case No: 122-cv-607 (E.D. Va. 2022) (Trenga, J.); and *Microsoft, Fortra, and Health-ISAC v. John Does 1-16*, Case No. 23-cv-2447 (E.D.N.Y 2023) (DeArcy Hall, J.). Although Plaintiffs have previously sought *ex parte* relief against other cybercriminal organizations, Plaintiffs have not previously sought this particular *ex parte* relief in this district as to these particular Defendants—the John Does who operate the Star Blizzard cybercriminal organization.

6. Plaintiffs have identified certain Internet domains as part of the infrastructure of the Star Blizzard Defendants. The domains associated with the Star Blizzard Defendants' infrastructure and the contact information for registrants of the domains are set forth at **Appendix A** to the Complaint. A true and correct copy of **Appendix A** to the Complaint is attached hereto as **Exhibit 1**.

7. Investigators of Microsoft's Digital Crimes Unit, including Sean Ensz who has provided a declaration in support of Plaintiffs' TRO Application, have worked to determine the true identities of the Star Blizzard Defendants. The only publicly available contact information or identifying information associated with the Star Blizzard Defendants are the email addresses they used to register the domains that form the Star Blizzard technical infrastructure. Based on our prior experience, it is likely that other contact information has been provided by the Star Blizzard Defendants to the Internet domain name registrars during the domain name registration and maintenance process, including, for example, individual and entity names, physical addresses, email addresses, facsimile numbers, telephone numbers, or payment information.

8. Based on ourexperience, the email addresses provided to the domain registrars are most likely to be the most accurate contact information. This is because while the name,

physical address, or phone numbers provided by the Star Blizzard Defendants may be purposefully false to obfuscate their identities—which given the Star Blizzard Defendants' criminal activity is unsurprising that they would go to lengths to mask their identities—the Star Blizzard Defendants are more likely to use real emails address in connection with the registration efforts. When registrants (the individual or entity who signs up and pays for a website domain; here the Star Blizzard Defendants) set up website domains and associated infrastructure they must receive confirmation from the Internet domain registrars via email in order to utilize and access the Internet domains. In past experiences relating to botnets, we have observed that the name, physical address, or telephone number were determined to be fraudulent or stolen, but the email address provided by defendants was, in fact, associated with them. Further supporting this conclusion, in May 2010, the Internet Corporation for Assigned Names and Numbers ("ICANN")—an organization that administers the domain name system—issued a study indicating the ease with which name and physical mailing addresses for domain registrations may be falsified. Attached hereto as **Exhibit 2** is a true and correct copy of the ICANN's May 2010 study, "WHOIS Proxy/Privacy Service Abuse – Definition."

9. Based on our prior experience and from Plaintiffs' research, I believe that the most reliable contact information for effecting communication with the Star Blizzard Defendants are email addresses that have been discovered to be associated with the Star Blizzard Defendants domains, and the contact information, particularly email addresses, in possession of the Internet domain registrars. From on our research, I conclude that such contact information is likely to be valid, as it is necessary to obtain Internet domain names or web hosting service. Upon provision of such contact information by the Internet domain registrars and web hosting companies to Plaintiffs, notice of this proceeding and service of

process may be attempted using such contact information. Through our research, I have not discovered any other information that would enable, at this point, further identification of or contact with Star Blizzard Defendants other than that in the possession of these companies. I believe that absent an order directing Doe discovery, these companies will be unlikely to share contact information necessary to provide notice and service to the Star Blizzard Defendants.

II. NOTICE AND SERVICE OF PROCESS

A. Plaintiffs Have Robust Plans To Provide Notice

10. On behalf of Plaintiffs, Crowell will attempt notice of any TRO and preliminary injunction hearing, as well as service of the Complaint by sending the pleadings and/or links to the pleadings to e-mail addresses, facsimile numbers and mailing addresses associated with the Star Blizzard Defendants or otherwise provided by the Star Blizzard Defendants to the domain registrars.

11. On behalf of Plaintiffs, Crowell will attempt notice of any TRO, preliminary injunction hearing and service of the Complaint by publishing those pleadings on a publicly accessible website located at: www.noticeofpleadings.com/starblizzard. Crowell will publish such notice on the website for the duration of this litigation. The following information will be made available on the website:

a. The information contained in the case caption and the content of the summons.

b. The following summary statement of the object of the complaint and the demand for relief: "Plaintiffs Microsoft Corporation ("Microsoft") and NGO Information Sharing and Analysis Center ("NGO-ISAC") have sued Defendants John Does 1-2 associated with the Star Blizzard cybercriminal operation and domains listed in the documents set forth herein. Plaintiffs allege that the Star Blizzard Defendants have violated Federal and state law by hosting a cybercriminal operation through these domains, orchestrating a sophisticated spear phishing operation, impersonating victims and victims' contacts to trick the victim into sharing login credentials, using the login credentials to infiltrate email systems, and exfiltrating sensitive

personal and commercial data and have committed intellectual property violations to the injury of Plaintiffs and Plaintiffs' customers and member organizations. Plaintiffs seek a preliminary injunction directing the registrars associated with these domains to take all steps necessary to disable access to and operation of these domains to ensure that changes or access to the domains cannot be made absent a court order and that all content and material associated with these domains are to be isolated and preserved pending resolution of the dispute. Plaintiffs seek a permanent injunction, other equitable relief and damages. Full copies of the pleading documents are available at www.noticeofpleadings.com/starblizzard.

c. The date of first publication.

d. The following text: "NOTICE TO DEFENDANT: READ THESE PAPERS CAREFULLY! You must "appear" in this case or the other side will win automatically. To "appear" you must file with the court a legal document called a "motion" or "answer." The "motion" or "answer" must be given to the court clerk or administrator within 21 days of the date of first publication specified herein. It must be in proper form and have proof of service on the Plaintiffs' attorneys, Jeffrey L. Poston at Crowell & Moring LLP, 1001 Pennsylvania Avenue NW, Washington D.C. 20004, jposton@crowell.com. If you have questions, you should consult with your own attorney immediately."

12. On behalf of Plaintiffs, Crowell will serve each of the Internet domain registries listed at **Appendix A** to the Complaint with all copies of all documents served on the Star Blizzard Defendants.

13. On behalf of Plaintiffs, Crowell will also attempt notice of any TRO and preliminary injunction hearing, as well as service of the complaint by personal delivery on any Defendant in this case that has provided existing physical addresses in the United States.

14. On behalf of Plaintiffs, to the extent the identity of the Star Blizzard John Doe Defendants become known to Plaintiffs, Crowell will prepare Requests for Service Abroad of Judicial or Extrajudicial Documents to attempt notice of any TRO and preliminary injunction hearing, as well as service of the Complaint on any Star Blizzard Defendants in this case that have provided contact information in foreign countries that are signatories to the Hague Convention on Service Abroad or any similar treaty, and will comply with the requirements

of those treaties. Upon entry of any TRO, Crowell will execute and deliver these documents to the appropriate Central Authority and request, pursuant to the Hague Convention or similar treaty, that the Central Authority deliver these documents to the contact information provided by the Star Blizzard Defendants. I am informed, and therefore believe, that notice of the preliminary injunction hearing and service of the Complaint could take approximately three to six months or longer through this process.

B. Notice Under ICANN Domain Name Registration Policies

15. Attached hereto as **Exhibit 3** is a true and correct copy of a document describing ICANN's role. Exhibit 3 reflects the following: ICANN is a not-for-profit partnership formed in 1998. ICANN coordinates domain names and IP addresses (unique identifying numbers for computers throughout the world), which enables the operation of the global Internet. ICANN's responsibilities include running an accreditation system for domain name "registrars." Domain name registrars enter into arrangements with individual "registrants" who wish to register particular domain names. ICANN has a contractual relationship with all accredited registrars that set forth the registrars' obligations. The purpose of the requirements of ICANN's accreditation agreements with registrars is to provide a consistent and stable environment for the domain name system, and hence the Internet.

16. A true and correct copy of the 2013 ICANN Registrar Accreditation Agreement between ICANN and domain name registrars is attached hereto as **Exhibit 4**.

17. The following summarizes provisions set forth in the ICANN accreditation agreements with registrars at Exhibit 4.

ICANN Requires That Registrants Agree To Provide Accurate Contact Information

18. Section 3.7.7.1 of the accreditation agreement provides that domain registrants will provide the registrar accurate and reliable contact information. In particular, the domain name

registrant:

> "shall provide to Registrar accurate and reliable contact details and correct and update them within seven (7) days of any change during the term of the Registered Name registration, including: the full name, postal address, e-mail address, voice telephone number, and fax number if available of the Registered Name Holder; name of authorized person for contact purposes in the case of an Registered Name Holder that is an organization, association, or corporation…."

19. Section 3.7.7.2 of the accreditation agreement provides that if the registrant fails to respond for over 15 days to a registrar's inquiry about inaccurate contact information, the domain may be cancelled. In particular, the domain name registrant's:

> "willful provision of inaccurate or unreliable information, its willful failure to update information provided to Registrar within seven (7) days of any change, or its failure to respond for over fifteen (15) days to inquiries by Registrar concerning the accuracy of contact details associated with the Registered Name Holder's registration shall constitute a material breach of the Registered Name Holder-registrar contract and be a basis for suspension and/or cancellation of the Registered Name registration."

ICANN Requires That Registrants Agree To A Dispute Resolution Policy Under Which Notice Is Given By Sending The Complaint To The Registrant's Contact Information

20. Section 3.8 of the accreditation agreement provides that registrars shall require registrants to agree to the Uniform Domain Name Dispute Resolution Policy ("UDRP"). The UDRP is a policy between a registrar and its customer and is included in registration agreements for all ICANN-accredited registrars. Attached hereto as **Exhibit 5** is a true and correct copy of the UDRP.

21. As part of the registrant's agreement to the UDRP, the registrant agrees to the Rules for Uniform Domain Name Dispute Resolution Policy ("Rules"). Attached hereto as **Exhibit 6** is a true and correct copy of the Rules.

22. Pursuant to the Rules, "Written Notice" of a complaint regarding a domain requires electronic transmittal of the complaint to a domain registrant and hardcopy notification that the

complaint was sent by electronic means. In particular, "Written Notice" is defined as:

> "hardcopy notification by the Provider to the Respondent of the commencement of an administrative proceeding under the Policy which shall inform the respondent that a complaint has been filed against it, and which shall state that the Provider has electronically transmitted the complaint including any annexes to the Respondent by the means specified herein. Written notice does not include a hardcopy of the complaint itself or any annexes."

23. Pursuant to the Rules, notice of a complaint may be achieved by the registrar forwarding the complaint to the postal address, facsimile number and e-mail addresses of the domain registrant. In particular, the Rules define the procedure for providing notice as follows:

> "(a) When forwarding a complaint, including any annexes, electronically to the Respondent, it shall be the Provider's responsibility to employ reasonably available means calculated to achieve actual notice to Respondent. Achieving actual notice, or employing the following measures to do so, shall discharge this responsibility:
>
> (i) sending Written Notice of the complaint to all postal-mail and facsimile addresses (A) shown in the domain name's registration data in Registrar's Whois database for the registered domain-name holder, the technical contact, and the administrative contact and (B) supplied by Registrar to the Provider for the registration's billing contact; and
>
> (ii) sending the complaint, including any annexes, in electronic form by e-mail to:
>
> (A) the e-mail addresses for those technical, administrative and billing contacts;
>
> (B) postmaster@<the contested domain name>; and
>
> (C) if the domain name (or "www." followed by the domain name) resolves to an active web page other than a generic page the Provider concludes is maintained by a registrar or ISP for parking domain-names registered by multiple domain-name holders), any e-mail address shown or e-mail links on that web page; and
>
> (iii) sending the complaint, including any annexes, to any e-

> mail address the Respondent has notified the Provider it prefers and, to the extent practicable, to all other e-mail addresses provided to the Provider by Complainant..."

24. The effect of the UDRP and the Rules is that domain name registrants agree that notice of a complaint relating to their domains may be provided by the foregoing means, including by sending the complaint to postal, facsimile and email addresses provided by registrants.

ICANN Requires That Registrants Agree That Domains May Be Suspended Or Cancelled Pursuant To The Dispute Resolution Policy

25. Section 3.7.7.11 of the accreditation agreement provides that registrars shall require that a domain name registrant "shall agree that its registration of the Registered Name shall be subject to suspension, cancellation, or transfer" pursuant to ICANN's policies for the resolution of disputes concerning domain names.

ICANN Requires That Registrants Agree Not To Use Domains In An Illegal Manner

26. Under Section 2 of the UDRP, the domain registrant agrees that:

> "By applying to register a domain name, or by asking us to maintain or renew a domain name registration, you hereby represent and warrant to us that (a) the statements that you made in your Registration Agreement are complete and accurate; (b) to your knowledge, the registration of the domain name will not infringe upon or otherwise violate the rights of any third party; (c) you are not registering the domain for an unlawful purpose; and (d) you will not knowingly use the domain name in violation of any applicable laws or regulations. It is your responsibility to determine whether your domain name registration infringes or violates someone else's rights."

27. Similarly, Section 3.7.7.9 of the accreditation agreement provides that the domain name registrant "shall represent that, to the best of the Registered Name Holder's knowledge and belief, neither the registration of the Registered Name nor the manner in which it is directly or indirectly used infringes the legal rights of any third party."

The Star Blizzard Defendants' Internet Domain Registrars Send Account-Related Information To Customer-Provided Contacts

28. The terms of service for Internet domain registrars used by the Star Blizzard Defendants provide that their customers must provide contact information, including the email address, postal address, and a valid telephone number where they can reach their customers. These Internet domain registrars further provide that they may contact their respective customers based on the information provided by that customer. In particular, NameSilo, LLC's ("NameSilo") General Terms and Conditions, available at https://www.namesilo.com/Support/General-Terms-and-Conditions, include such provisions. Similarly, Key-Systems GmbH's ("Key-Systems") Registration Agreement, available at https://www.key-systems.net/en/registration-agreement, also includes such provisions. A true and correct copy of each NameSilo's General Terms and Conditions and Key-Systems' Registration Agreement are attached hereto as **Exhibit 7**.

29. Based on our past experience and our research of third parties that the Star Blizzard Defendants use to provide domain name services, the other third party Internet domain name registrars require that similar contact information be provided.

The Star Blizzard Defendants' Internet Domain Name Registrars' Terms Of Service Prohibit Customers From Using Services In An Illegal Manner

30. The Internet domain registrars' terms of service prohibit customers, including the Star Blizzard Defendants, from using the services in an illegal manner, and customer accounts may be terminated for violation of those terms. For example, NameSilo's agreement prohibits, among other conduct, the registered domain being used to:

a. registration of prohibited domain name(s),

b. abuse of NameSilo's services,

c. payment irregularities,

d. illegal conduct,

e. failure to keep account or WHOIS information accurate and up to date,

f. failure to respond to inquiries from NameSilo for over three (3) calendar days,

g. if use of NameSilo's services involves NameSilo in a violation of any third party's rights or acceptable use policies, including but not limited to the transmission of unsolicited email, the violation of any copyright, or the distribution of any form of malware (defined to include, without limitation, malicious code or software that might affect the operation of the Internet),

h. to comply with any applicable court orders, laws, government rules or requirements, requests of law enforcement or other governmental agency or organization, or any dispute resolution process,

i. to avoid any liability, civil or criminal, on the part of NameSilo, as, well as its affiliates, subsidiaries, officers, directors, and employees,

j. to protect the integrity, security and stability of the Domain Name system (DNS), or

k. failure to respond to inquiries from NameSilo regarding payment inquiries for over 24 hours

31. NameSilo's policies also provide that it may suspend or terminate its customer's services if that customer has been found to engage in prohibited conduct. Based on my past experience and my current research of other Internet domain registrars, and on information and belief, the other Internet domain registrars used by the Star Blizzard Defendants prohibit similar unlawful conduct.

III. OTHER AUTHORITY AND EVIDENCE

32. The requested *ex parte* relief Plaintiffs seek has been granted against similarly situated cybercriminal organizations in the past. Additionally, Plaintiffs' proposed alternative service has previously been granted in other actions brought by Microsoft to halt other cybercriminal organizations that, like the Star Blizzard Defendants, carryout their unlawful activity through the use of a technical infrastructure using Internet domains.

33. Attached hereto as **Exhibit 8** is a true and correct copy of the March 15, 2019

Ex Parte Temporary Restraining Order and Order To Show Cause in the matter of *Microsoft v. John Does 1-2*, Case No. 1:19-cv-00716-ABJ (D.C. 2019) (Berman-Jackson, J.).

34. Attached hereto as **Exhibit 9** is a true and correct copy of the December 18, 2019 *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Microsoft v. John Does 1-2,* Case No. 1:19-cv-01582 (E.D. Va. 2019) (O'Grady, J.).

35. Attached hereto as **Exhibit 10** is a true and correct copy of the May 1, 2020 *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Sophos v. John Does 1*-2, Case No. 1:20-cv-00502 (E.D. Va. 2020) (O'Grady, J.).

36. Attached hereto as **Exhibit 11** is a true and correct copy of the July 1, 2020 *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Microsoft v. John Does 1-2,* Case No. 1:20-cv-00730 (E.D. Va. 2020) (O'Grady, J.).

37. Attached hereto as **Exhibit 12** is a true and correct copy of the July 22, 2020 *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *DXC Technology Company v. John Does 1-2,* Case No. 1:20-cv-00814 (E.D. Va. 2020) (Alston, J.).

38. Attached hereto as **Exhibit 13** is a true and correct copy of the October 6, 2020 *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Microsoft and FS-ISAC v. John Does 1-2,* Case No. 1:20-cv-1171 (E.D. Va. 2020) (Trenga, J.).

39. Attached hereto as **Exhibit 14** is a true and correct copy of the April 8, 2022 *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Microsoft, FS-ISAC, and Health-ISAC v. Malikov et al.*, Case No. 1:22-cv-1328 (N. D. Ga. 2022) (Cohen, J.)

40. Attached hereto as **Exhibit 15** is a true and correct copy of the May 27, 2022 *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Microsoft*

v. John Does 1-2, Case No: 122-cv-607 (E.D. Va. 2022) (Trenga, J.)

41. Attached hereto as **Exhibit 16** is a true and correct copy of the *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Microsoft, Fortra, and Health-ISAC v. John Does 1-16*, Case No. 23-cv-2447 (E.D.N.Y 2023) (Morrison, J.)

42. In each of the cases identified in the foregoing paragraphs, the Court granted similar *ex parte relief* to takedown the cybercriminal operation's technical infrastructure and authorized alternative service as requested here.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed this 24th day of September, 2024 in Washington D.C.

Jeffrey L. Poston

Jeffrey L. Poston

APPENDIX A

.COM REGISTRY
VeriSign Global Registry Services
12061 Bluemont Way
Reston VA 20190

.COM DOMAIN

ANKARAMUHASEBEN.COM	Domain Name: ANKARAMUHASEBEN.COM Registry Domain ID: 2859614504_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2024-02-29T16:32:16Z Creation Date: 2024-02-29T16:32:13Z Registry Expiry Date: 2025-02-28T16:32:13Z Registrar: NameCheap, Inc. Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: DNS1.REGISTRAR-SERVERS.COM Name Server: DNS2.REGISTRAR-SERVERS.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2024-09-20T17:17:01Z <<<
BIGDATABROADWAY.COM	Domain name: BIGDATABROADWAY.COM Registry Domain ID: 2856022843_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2024-02-17T18:27:19.00Z Registrar Registration Expiration Date: 2025-02-17T18:27:19.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy

	Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: cad10b04e802496cb7f315f443084ac1.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: cad10b04e802496cb7f315f443084ac1.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: cad10b04e802496cb7f315f443084ac1.protect@withheldforprivacy.com

	Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-20T16:20:25.39Z <<<
CLOUDDEFSYSTEMS.COM	Domain name: clouddefsystems.com Registry Domain ID: 2764044774_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-03-10T08:39:33.00Z Registrar Registration Expiration Date: 2024-03-10T08:39:33.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 94ac459a70de4e3bb65db311eea9da56.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region

	Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 94ac459a70de4e3bb65db311eea9da56.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 94ac459a70de4e3bb65db311eea9da56.protect@withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ For more information on Whois status codes, please visit https://icann.org/epp
CLOUDINFODATA.COM	Domain name: cloudinfodata.com Registry Domain ID: 2781367380_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-05-16T15:23:52.00Z Registrar Registration Expiration Date: 2024-05-16T15:23:52.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC

	Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: REACTIVATION PERIOD Registrant Organization: Withheld for Privacy Purposes Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: reactivation-pending@mail.withheldforprivacy.com Registry Admin ID: Admin Name: REACTIVATION PERIOD Admin Organization: Withheld for Privacy Purposes Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: reactivation-pending@mail.withheldforprivacy.com Registry Tech ID: Tech Name: REACTIVATION PERIOD Tech Organization: Withheld for Privacy Purposes Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: reactivation-pending@mail.withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com

	DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ For more information on Whois status codes, please visit https://icann.org/epp
CLOUDITHUB.COM	omain name: cloudithub.com Registry Domain ID: 2784305716_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2024-06-26T01:43:42.64Z Creation Date: 2023-05-26T16:28:35.00Z Registrar Registration Expiration Date: 2025-05-26T16:28:35.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 723eed6a6b98418d905c68cebf3d06be.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS

	Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 723eed6a6b98418d905c68cebf3d06be.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 723eed6a6b98418d905c68cebf3d06be.protect@withheldforprivacy.com Name Server: ns1.dan.com Name Server: ns2.dan.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ For more information on Whois status codes, please visit https://icann.org/epp
DATAWEBHUB.COM	Domain name: datawebhub.com Registry Domain ID: 2784305714_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2024-06-26T01:46:46.46Z Creation Date: 2023-05-26T16:28:34.00Z Registrar Registration Expiration Date: 2025-05-26T16:28:34.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

	Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: bb1402f4bbb14246947e77ef4598aae0.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: bb1402f4bbb14246947e77ef4598aae0.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext:

	Tech Email: bb1402f4bbb14246947e77ef4598aae0.protect@withheldforprivacy.com Name Server: ns1.dan.com Name Server: ns2.dan.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
DOCSECGATE.COM	Domain Name: DOCSECGATE.COM Registry Domain ID: 2797453581_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2024-08-22T13:39:52Z Creation Date: 2023-07-11T13:27:59Z Registry Expiry Date: 2024-07-11T13:27:59Z Registrar: NameCheap, Inc. Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: redemptionPeriod https://icann.org/epp#redemptionPeriod Name Server: DNS101.REGISTRAR-SERVERS.COM Name Server: DNS102.REGISTRAR-SERVERS.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2024-09-20T17:25:49Z <<<
E-FLUXXSOLUTIONS.COM	Domain name: e-fluxxsolutions.com Registry Domain ID: 2775421497_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-04-24T10:42:21.00Z Registrar Registration Expiration Date: 2024-04-24T10:42:21.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC

	Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: b115c8ed61ca4385bde370956ce374d8.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: b115c8ed61ca4385bde370956ce374d8.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax:

	Tech Fax Ext: Tech Email: b115c8ed61ca4385bde370956ce374d8.protect@withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ For more information on Whois status codes, please visit https://icann.org/epp
ENTHEOGENICMD.COM	Domain Name: ENTHEOGENICMD.COM Registry Domain ID: 2894098537_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.hostinger.com Registrar URL: http://www.hostinger.com Updated Date: 2024-06-26T13:54:05Z Creation Date: 2024-06-26T13:53:58Z Registry Expiry Date: 2025-06-26T13:53:58Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636 Registrar Abuse Contact Email: abuse-tracker@hostinger.com Registrar Abuse Contact Phone: +37064503378 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: NS1.DNS-PARKING.COM Name Server: NS2.DNS-PARKING.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2024-09-20T17:30:06Z <<<
EXTRACTORDRAW.COM	Domain Name: EXTRACTORDRAW.COM Registry Domain ID: 2863506875_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.hostinger.com Registrar URL: http://www.hostinger.com Updated Date: 2024-03-14T17:31:07Z Creation Date: 2024-03-14T17:31:02Z Registry Expiry Date: 2025-03-14T17:31:02Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636 Registrar Abuse Contact Email: abuse-tracker@hostinger.com Registrar Abuse Contact Phone: +37064503378

	Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: NS1.DNS-PARKING.COM Name Server: NS2.DNS-PARKING.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2024-09-20T17:31:22Z <<<
GALETSCRYPTODATA.COM	Domain name: galetscryptodata.com Registry Domain ID: 2760849968_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-02-24T18:49:12.00Z Registrar Registration Expiration Date: 2024-02-24T18:49:12.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 1938c38cd84245458600905600 2f69dc.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf

	Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 1938c38cd84245458600905600 2f69dc.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 1938c38cd84245458600905600 2f69dc.protect@withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ For more information on Whois status codes, please visit https://icann.org/epp
GATEBLURBREPOSITORY.COM	Domain Name: GATEBLURBREPOSITORY.COM Registry Domain ID: 2759139284_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2024-08-24T22:01:34Z Creation Date: 2023-02-17T18:02:46Z Registry Expiry Date: 2025-02-17T18:02:46Z Registrar: NameCheap, Inc. Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com

	Registrar Abuse Contact Phone: +1.6613102107 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: NS1.DAN.COM Name Server: NS2.DAN.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2024-09-20T17:35:56Z <<<
GATEWAYDOCSINT.COM	Domain name: gatewaydocsint.com Registry Domain ID: 2754772928_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-01-29T21:32:39.00Z Registrar Registration Expiration Date: 2025-01-29T21:32:39.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Redacted for Privacy Purposes Registrant Name: Redacted for Privacy Purposes Registrant Organization: Redacted for Privacy Purposes Registrant Street: Redacted for Privacy Purposes Registrant City: Redacted for Privacy Purposes Registrant State/Province: FL Registrant Postal Code: Redacted for Privacy Purposes Registrant Country: US Registrant Phone: Redacted for Privacy Purposes Registrant Phone Ext: Redacted for Privacy Purposes Registrant Fax: Redacted for Privacy Purposes Registrant Fax Ext: Redacted for Privacy Purposes Registrant Email: Select Contact Domain Holder link at https://www.namecheap.com/domains/whois/result?domain=gatewaydocsint.com Registry Admin ID: Redacted for Privacy Purposes Admin Name: Redacted for Privacy Purposes Admin Organization: Redacted for Privacy Purposes Admin Street: Redacted for Privacy Purposes Admin City: Redacted for Privacy Purposes

	Admin State/Province: Redacted for Privacy Purposes Admin Postal Code: Redacted for Privacy Purposes Admin Country: Redacted for Privacy Purposes Admin Phone: Redacted for Privacy Purposes Admin Phone Ext: Redacted for Privacy Purposes Admin Fax: Redacted for Privacy Purposes Admin Fax Ext: Redacted for Privacy Purposes Admin Email: Select Contact Domain Holder link at https://www.namecheap.com/domains/whois/result?domain=gatewaydocsint.com Registry Tech ID: Redacted for Privacy Purposes Tech Name: Redacted for Privacy Purposes Tech Organization: Redacted for Privacy Purposes Tech Street: Redacted for Privacy Purposes Tech City: Redacted for Privacy Purposes Tech State/Province: Redacted for Privacy Purposes Tech Postal Code: Redacted for Privacy Purposes Tech Country: Redacted for Privacy Purposes Tech Phone: Redacted for Privacy Purposes Tech Phone Ext: Redacted for Privacy Purposes Tech Fax: Redacted for Privacy Purposes Tech Fax Ext: Redacted for Privacy Purposes Tech Email: Select Contact Domain Holder link at https://www.namecheap.com/domains/whois/result?domain=gatewaydocsint.com Name Server: ns1.dan.com Name Server: ns2.dan.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-19T22:38:23.64Z <<<
GAWECRYPTOINFOSOLUTIONS.COM	Domain name: gawecryptoinfosolutions.com Registry Domain ID: 2760849980_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-02-24T18:49:17.00Z Registrar Registration Expiration Date: 2024-02-24T18:49:17.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC

	Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 820478c363754e72bad77cc0e5a20663.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 820478c363754e72bad77cc0e5a20663.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax:

	Tech Fax Ext: Tech Email: 820478c363754e72bad77cc0e5a20663.protect@withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ For more information on Whois status codes, please visit https://icann.org/epp
GETFIGMACREATOR.COM	Domain name: GETFIGMACREATOR.COM Registry Domain ID: 2805036851_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-08-11T13:13:20.00Z Registrar Registration Expiration Date: 2024-08-11T13:13:20.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: REACTIVATION PERIOD Registrant Organization: Withheld for Privacy Purposes Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: reactivation-pending@mail.withheldforprivacy.com Registry Admin ID: Admin Name: REACTIVATION PERIOD Admin Organization: Withheld for Privacy Purposes Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik

	Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: reactivation-pending@mail.withheldforprivacy.com Registry Tech ID: Tech Name: REACTIVATION PERIOD Tech Organization: Withheld for Privacy Purposes Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: reactivation-pending@mail.withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-19T18:41:32.94Z <<<
GOVSAFEBREAKTHROUGH.COM	Domain name: GOVSAFEBREAKTHROUGH.COM Registry Domain ID: 2797988434_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-07-13T16:26:44.00Z Registrar Registration Expiration Date: 2024-07-13T16:26:44.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

	Domain Status: pendingDelete https://icann.org/epp#pendingDelete Domain Status: redemptionPeriod https://icann.org/epp#redemptionPeriod Registry Registrant ID: Registrant Name: REACTIVATION PERIOD Registrant Organization: Withheld for Privacy Purposes Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: reactivation-pending@mail.withheldforprivacy.com Registry Admin ID: Admin Name: REACTIVATION PERIOD Admin Organization: Withheld for Privacy Purposes Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: reactivation-pending@mail.withheldforprivacy.com Registry Tech ID: Tech Name: REACTIVATION PERIOD Tech Organization: Withheld for Privacy Purposes Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: reactivation-pending@mail.withheldforprivacy.com

	Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-20T16:43:20.59Z <<<
GUARDITTECH.COM	Domain name: guarditttech.com Registry Domain ID: 2772370916_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-04-12T13:36:33.00Z Registrar Registration Expiration Date: 2024-04-12T13:36:33.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 7c57f044c47e45b5a673950a7861ba8b.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region

	Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 7c57f044c47e45b5a673950a7861ba8b.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 7c57f044c47e45b5a673950a7861ba8b.protect@withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ For more information on Whois status codes, please visit https://icann.org/epp
HELMETKUP.COM	Domain name: HELMETKUP.COM Registry Domain ID: 2859617771_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2024-02-29T17:04:27.00Z Registrar Registration Expiration Date: 2025-02-28T17:04:27.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC

	Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: b0f651910fc24e5cb826549a09331910.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: b0f651910fc24e5cb826549a09331910.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax:

	Tech Fax Ext: Tech Email: b0f651910fc24e5cb826549a09331910.protect@withheldforprivacy.com Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-20T09:44:28.70Z <<<
IMGRICH.COM	Domain Name: IMGRICH.COM Registry Domain ID: 2863761839_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.hostinger.com Registrar URL: http://www.hostinger.com Updated Date: 2024-03-15T14:56:16Z Creation Date: 2024-03-15T14:56:13Z Registry Expiry Date: 2025-03-15T14:56:13Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636 Registrar Abuse Contact Email: abuse-tracker@hostinger.com Registrar Abuse Contact Phone: +37064503378 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: NS1.DNS-PARKING.COM Name Server: NS2.DNS-PARKING.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2024-09-20T17:48:02Z <<<
INREALCONNECT.COM	Domain Name: INREALCONNECT.COM Registry Domain ID: 2870766541_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2024-04-09T14:49:24Z Creation Date: 2024-04-09T14:49:21Z Registry Expiry Date: 2025-04-09T14:49:21Z Registrar: NameCheap, Inc. Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107

	Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: DNS1.REGISTRAR-SERVERS.COM Name Server: DNS2.REGISTRAR-SERVERS.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2024-09-20T17:49:04Z <<<
INSTANTPOINTZERO.COM	Domain name: INSTANTPOINTZERO.COM Registry Domain ID: 2861020667_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2024-03-05T12:37:50.00Z Registrar Registration Expiration Date: 2025-03-05T12:37:50.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 9165fd17e3a24cedb27207ac20cbb972.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy

	Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 9165fd17e3a24cedb27207ac20cbb972.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 9165fd17e3a24cedb27207ac20cbb972.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-20T06:52:04.76Z <<<
INTELLIGENTAUTOMATIONALLEY.COM	Domain name: INTELLIGENTAUTOMATIONALLEY.COM Registry Domain ID: 2856020497_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2024-02-17T17:57:50.00Z

	Registrar Registration Expiration Date: 2025-02-17T17:57:50.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: e7c4de7cd08642b3a8c409c734a647d8.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: e7c4de7cd08642b3a8c409c734a647d8.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2

	Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: e7c4de7cd08642b3a8c409c734a647d8.protect@withheldforprivacy.com Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-20T02:54:16.18Z <<<
KEEPERDOCUMENTLLC.COM	Domain name: keeperdocumentllc.com Registry Domain ID: 2765526386_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-03-16T09:09:23.00Z Registrar Registration Expiration Date: 2024-03-16T09:09:23.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax:

	Registrant Fax Ext: Registrant Email: 242400c85b41476d846e8cc4a0b8f62d.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 242400c85b41476d846e8cc4a0b8f62d.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 242400c85b41476d846e8cc4a0b8f62d.protect@withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ For more information on Whois status codes, please visit https://icann.org/epp
KEEPERITLABEL.COM	Domain name: keeperitlabel.com

	Registry Domain ID: 2762230896_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-03-02T16:03:10.00Z Registrar Registration Expiration Date: 2024-03-02T16:03:10.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 75fa2915399b4e47abcf39c76a78b44f.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext:

	Admin Email: 75fa2915399b4e47abcf39c76a78b44f.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 75fa2915399b4e47abcf39c76a78b44f.protect@withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ For more information on Whois status codes, please visit https://icann.org/epp
LIQUIDACIONESJUDICIALES.COM	Domain Name: liquidacionesjudiciales.com Registry Domain ID: 2760466030_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.regtons.com Registrar URL: http://regtons.com Updated Date: 2024-02-23T00:00:00Z Creation Date: 2023-02-22T00:00:00Z Registrar Registration Expiration Date: 2025-02-22T00:00:00Z Registrar: GRANSY S.R.O D/B/A SUBREG.CZ Registrar IANA ID: 1505 Registrar Abuse Contact Email: abuse@regtons.com Registrar Abuse Contact Phone: +420.734463373 Domain Status: clienttransferprohibited https://www.icann.org/epp#clienttransferprohibited Registry Registrant ID: Not Disclosed Registrant Name: Not Disclosed Not Disclosed Registrant Organization: My Domain Provider Registrant Street: Not Disclosed Registrant City: Not Disclosed

	Registrant State/Province: Registrant Postal Code: Not Disclosed Registrant Country: NL Registrant Phone: Not Disclosed Registrant Phone Ext: Not Disclosed Registrant Fax: Not Disclosed Registrant Fax Ext: Not Disclosed Registrant Email: webproxy@whoisprotection.domains Registry Admin ID: Not Disclosed Admin Name: Not Disclosed Not Disclosed Admin Organization: Admin Street: Not Disclosed Admin City: Not Disclosed Admin State/Province: Not Disclosed Admin Postal Code: Not Disclosed Admin Country: Not Disclosed Admin Phone: Not Disclosed Admin Phone Ext: Not Disclosed Admin Fax: Not Disclosed Admin Fax Ext: Not Disclosed Admin Email: webproxy@whoisprotection.domains Registry Tech ID: Not Disclosed Tech Name: Not Disclosed Not Disclosed Tech Organization: Tech Street: Not Disclosed Tech City: Not Disclosed Tech State/Province: Not Disclosed Tech Postal Code: Not Disclosed Tech Country: Not Disclosed Tech Phone: Not Disclosed Tech Phone Ext: Not Disclosed Tech Fax: Not Disclosed Tech Fax Ext: Not Disclosed Tech Email: webproxy@whoisprotection.domains Name Server: suspension1.mydomainprovider.com Name Server: suspension2.mydomainprovider.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
MAYQUARKESTHETIC.COM	Domain Name: MAYQUARKESTHETIC.COM Registry Domain ID: 2870492494_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.hostinger.com Registrar URL: https://www.hostinger.com Updated Date: 2024-06-08T02:17:53Z Creation Date: 2024-04-08T17:00:35Z

	Registrar Registration Expiration Date: 2025-04-08T17:00:35Z Registrar: Hostinger Operations, UAB Registrar IANA ID: 1636 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: 10 Corporate Drive Registrant City: Burlington Registrant State/Province: MA Registrant Postal Code: 01803 Registrant Country: US Registrant Phone: +1.8022274003 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@privacyprotect.org Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: Privacy Protect, LLC (PrivacyProtect.org) Admin Street: 10 Corporate Drive Admin City: Burlington Admin State/Province: MA Admin Postal Code: 01803 Admin Country: US Admin Phone: +1.8022274003 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact@privacyprotect.org Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: Privacy Protect, LLC (PrivacyProtect.org) Tech Street: 10 Corporate Drive Tech City: Burlington Tech State/Province: MA Tech Postal Code: 01803 Tech Country: US Tech Phone: +1.8022274003 Tech Phone Ext: Tech Fax:

	Tech Fax Ext: Tech Email: contact@privacyprotect.org Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse@hostinger.com Registrar Abuse Contact Phone: +37064503378 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
METTEZERA.COM	Domain Name: METTEZERA.COM Registry Domain ID: 2894114626_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.hostinger.com Registrar URL: https://www.hostinger.com Updated Date: 2024-08-26T02:17:11Z Creation Date: 2024-06-26T16:33:04Z Registrar Registration Expiration Date: 2025-06-26T16:33:04Z Registrar: Hostinger Operations, UAB Registrar IANA ID: 1636 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: 10 Corporate Drive Registrant City: Burlington Registrant State/Province: MA Registrant Postal Code: 01803 Registrant Country: US Registrant Phone: +1.8022274003 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@privacyprotect.org Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: Privacy Protect, LLC (PrivacyProtect.org) Admin Street: 10 Corporate Drive Admin City: Burlington Admin State/Province: MA Admin Postal Code: 01803 Admin Country: US Admin Phone: +1.8022274003

	Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact@privacyprotect.org Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: Privacy Protect, LLC (PrivacyProtect.org) Tech Street: 10 Corporate Drive Tech City: Burlington Tech State/Province: MA Tech Postal Code: 01803 Tech Country: US Tech Phone: +1.8022274003 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@privacyprotect.org Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse@hostinger.com Registrar Abuse Contact Phone: +37064503378 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-20T17:59:47Z <<<
MURODJONOVS.COM	Domain Name: MURODJONOVS.COM Registry Domain ID: 2890773051_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.hostinger.com Registrar URL: https://www.hostinger.com Updated Date: 2024-08-15T02:17:11Z Creation Date: 2024-06-15T16:27:23Z Registrar Registration Expiration Date: 2025-06-15T16:27:23Z Registrar: Hostinger Operations, UAB Registrar IANA ID: 1636 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: 10 Corporate Drive Registrant City: Burlington

	Registrant State/Province: MA Registrant Postal Code: 01803 Registrant Country: US Registrant Phone: +1.8022274003 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@privacyprotect.org Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: Privacy Protect, LLC (PrivacyProtect.org) Admin Street: 10 Corporate Drive Admin City: Burlington Admin State/Province: MA Admin Postal Code: 01803 Admin Country: US Admin Phone: +1.8022274003 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact@privacyprotect.org Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: Privacy Protect, LLC (PrivacyProtect.org) Tech Street: 10 Corporate Drive Tech City: Burlington Tech State/Province: MA Tech Postal Code: 01803 Tech Country: US Tech Phone: +1.8022274003 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@privacyprotect.org Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse@hostinger.com Registrar Abuse Contact Phone: +37064503378 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
OSOMTOYS.COM	Domain Name: OSOMTOYS.COM Registry Domain ID: 2774429345_DOMAIN_COM-VRSN

	Registrar WHOIS Server: whois.ownregistrar.com Registrar URL: http://www.ownregistrar.com Updated Date: 2024-04-21T07:07:45Z Creation Date: 2023-04-20T08:04:32Z Registry Expiry Date: 2025-04-20T08:04:32Z Registrar: OwnRegistrar, Inc. Registrar IANA ID: 1250 Registrar Abuse Contact Email: Registrar Abuse Contact Phone: Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: NS1.CR25.MANAGEDNS.ORG Name Server: NS2.CR25.MANAGEDNS.ORG DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
OWAORGANIZESPACE.COM	Domain name: owaorganizespace.com Registry Domain ID: 2750404096_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-01-10T15:33:26.00Z Registrar Registration Expiration Date: 2024-01-10T15:33:26.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext:

	Registrant Email: fbf088d1456b4705bf347ad8cd8af164.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: fbf088d1456b4705bf347ad8cd8af164.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: fbf088d1456b4705bf347ad8cd8af164.protect@withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ For more information on Whois status codes, please visit https://icann.org/epp
POSTREQUESTIN.COM	Domain name: postrequestin.com Registry Domain ID: 2805036855_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com

	Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-08-11T13:13:23.00Z Registrar Registration Expiration Date: 2024-08-11T13:13:23.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: REACTIVATION PERIOD Registrant Organization: Withheld for Privacy Purposes Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: reactivation-pending@mail.withheldforprivacy.com Registry Admin ID: Admin Name: REACTIVATION PERIOD Admin Organization: Withheld for Privacy Purposes Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: reactivation-pending@mail.withheldforprivacy.com Registry Tech ID: Tech Name: REACTIVATION PERIOD Tech Organization: Withheld for Privacy Purposes Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region

	Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: reactivation-pending@mail.withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
PROFFSOLUTION.COM	Domain name: proffsolution.com Registry Domain ID: 2781360245_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-05-16T14:20:42.00Z Registrar Registration Expiration Date: 2024-05-16T14:20:42.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: d3d1189d859748a39e4705e5c3eb7563.protect@withheldforprivacy.com Registry Admin ID:

	Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: d3d1189d859748a39e4705e5c3eb7563.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: d3d1189d859748a39e4705e5c3eb7563.protect@withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ For more information on Whois status codes, please visit https://icann.org/epp
PROTECTORDOCUMENTCENTER.COM	Domain name: protectordocumentcenter.com Registry Domain ID: 2765526395_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-03-16T09:09:27.00Z

	Registrar Registration Expiration Date: 2024-03-16T09:09:27.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: b1b68209f55246fdbce545ee00e76782.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: b1b68209f55246fdbce545ee00e76782.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2

	Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: b1b68209f55246fdbce545ee00e76782.protect@withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ For more information on Whois status codes, please visit https://icann.org/epp
PUREAFRO.COM	Domain Name: PUREAFRO.COM Registry Domain ID: 1544497306_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.tucows.com Registrar URL: http://www.tucows.com Updated Date: 2024-09-02T16:38:02Z Creation Date: 2009-02-27T09:26:23Z Registry Expiry Date: 2025-02-27T09:26:23Z Registrar: Tucows Domains Inc. Registrar IANA ID: 69 Registrar Abuse Contact Email: domainabuse@tucows.com Registrar Abuse Contact Phone: +1.4165350123 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: GAIL.NS.CLOUDFLARE.COM Name Server: NORMAN.NS.CLOUDFLARE.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2024-09-20T19:29:28Z <<<
RISEUPBIT.COM	Domain name: riseupbit.com Registry Domain ID: 2837954116_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com

	Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-12-15T17:32:12.00Z Registrar Registration Expiration Date: 2024-12-15T17:32:12.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: f193dbb5779c4ab995104643badb8655.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: f193dbb5779c4ab995104643badb8655.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy

	Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: f193dbb5779c4ab995104643badb8655.protect@withheldforprivacy.com Name Server: ns1.timeweb.ru Name Server: ns2.timeweb.ru Name Server: ns3.timeweb.org Name Server: ns4.timeweb.org DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-20T15:30:42.89Z <<<
SECLAWDOORWAY.COM	Domain name: SECLAWDOORWAY.COM Registry Domain ID: 2798235248_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-07-14T15:28:39.00Z Registrar Registration Expiration Date: 2024-07-14T15:28:39.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: pendingDelete https://icann.org/epp#pendingDelete Domain Status: redemptionPeriod https://icann.org/epp#redemptionPeriod Registry Registrant ID: Registrant Name: REACTIVATION PERIOD Registrant Organization: Withheld for Privacy Purposes

	Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: reactivation-pending@mail.withheldforprivacy.com Registry Admin ID: Admin Name: REACTIVATION PERIOD Admin Organization: Withheld for Privacy Purposes Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: reactivation-pending@mail.withheldforprivacy.com Registry Tech ID: Tech Name: REACTIVATION PERIOD Tech Organization: Withheld for Privacy Purposes Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: reactivation-pending@mail.withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-19T22:32:36.22Z <<<

SETUPPROFI.COM	Domain name: setupprofi.com Registry Domain ID: 2780256398_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-05-12T15:35:52.00Z Registrar Registration Expiration Date: 2024-05-12T15:35:52.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 309d713534bb4d579cb3d520a42b69fa.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext:

	Admin Email: 309d713534bb4d579cb3d520a42b69fa.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 309d713534bb4d579cb3d520a42b69fa.protect@withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ For more information on Whois status codes, please visit https://icann.org/epp
SKELETCHECK.COM	Domain Name: SKELETCHECK.COM Registry Domain ID: 2863745777_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.hostinger.com Registrar URL: https://www.hostinger.com Updated Date: 2024-05-15T02:16:44Z Creation Date: 2024-03-15T12:17:37Z Registrar Registration Expiration Date: 2025-03-15T12:17:37Z Registrar: Hostinger Operations, UAB Registrar IANA ID: 1636 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: 10 Corporate Drive Registrant City: Burlington Registrant State/Province: MA

	Registrant Postal Code: 01803 Registrant Country: US Registrant Phone: +1.8022274003 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@privacyprotect.org Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: Privacy Protect, LLC (PrivacyProtect.org) Admin Street: 10 Corporate Drive Admin City: Burlington Admin State/Province: MA Admin Postal Code: 01803 Admin Country: US Admin Phone: +1.8022274003 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact@privacyprotect.org Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: Privacy Protect, LLC (PrivacyProtect.org) Tech Street: 10 Corporate Drive Tech City: Burlington Tech State/Province: MA Tech Postal Code: 01803 Tech Country: US Tech Phone: +1.8022274003 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@privacyprotect.org Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse@hostinger.com Registrar Abuse Contact Phone: +37064503378 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-20T19:35:08Z <<<
SKYINFORMDATA.COM	Domain name: skyinformdata.com

	Registry Domain ID: 2779936825_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2024-06-11T01:51:10.59Z Creation Date: 2023-05-11T11:10:35.00Z Registrar Registration Expiration Date: 2025-05-11T11:10:35.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 1416e66ba6314846af7dc61b5becfb23.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext:

	Admin Email: 1416e66ba6314846af7dc61b5becfb23.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 1416e66ba6314846af7dc61b5becfb23.protect@withheldforprivacy.com Name Server: ns1.dan.com Name Server: ns2.dan.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-19T21:35:49.33Z <<<
STORAGEINFORMATIONSOLUTIONS.COM	Domain name: storageinformationsolutions.com Registry Domain ID: 2775716410_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-04-25T15:33:03.00Z Registrar Registration Expiration Date: 2024-04-25T15:33:03.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf

	Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 849a9c20eedf4ba6917e5e3b004b51f0.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 849a9c20eedf4ba6917e5e3b004b51f0.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 849a9c20eedf4ba6917e5e3b004b51f0.protect@withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com

	DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ For more information on Whois status codes, please visit https://icann.org/epp
TARIFJANE.COM	Domain Name: TARIFJANE.COM Registry Domain ID: 2806534838_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2024-08-18T07:19:27Z Creation Date: 2023-08-17T14:05:41Z Registry Expiry Date: 2025-08-17T14:05:41Z Registrar: NameCheap, Inc. Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: DNS101.REGISTRAR-SERVERS.COM Name Server: DNS102.REGISTRAR-SERVERS.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2024-09-20T19:37:47Z <<<
TRANSLATESPLIT.COM	Domain Name: TRANSLATESPLIT.COM Registry Domain ID: 2804793747_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2024-08-11T07:26:26Z Creation Date: 2023-08-10T16:47:53Z Registry Expiry Date: 2025-08-10T16:47:53Z Registrar: NameCheap, Inc. Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: DNS101.REGISTRAR-SERVERS.COM Name Server: DNS102.REGISTRAR-SERVERS.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

	>>> Last update of whois database: 2024-09-20T19:42:00Z <<<
VOCABPAPER.COM	Domain Name: VOCABPAPER.COM Registry Domain ID: 2863768341_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.hostinger.com Registrar URL: http://www.hostinger.com Updated Date: 2024-03-15T15:54:19Z Creation Date: 2024-03-15T15:54:15Z Registry Expiry Date: 2025-03-15T15:54:15Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636 Registrar Abuse Contact Email: abuse-tracker@hostinger.com Registrar Abuse Contact Phone: +37064503378 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: NS1.DNS-PARKING.COM Name Server: NS2.DNS-PARKING.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2024-09-20T19:43:45Z <<<
VOLTCLOUDPINE.COM	Domain Name: VOLTCLOUDPINE.COM Registry Domain ID: 2859317801_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2024-02-28T18:56:11Z Creation Date: 2024-02-28T18:35:17Z Registry Expiry Date: 2025-02-28T18:35:17Z Registrar: NameCheap, Inc. Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: NS1.DNS-PARKING.COM Name Server: NS2.DNS-PARKING.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2024-09-20T19:45:32Z <<<

WARDENGOVERMENTLAW.COM	Domain Name: WARDENGOVERMENTLAW.COM Registry Domain ID: 2798235251_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2024-08-25T15:39:46Z Creation Date: 2023-07-14T15:28:43Z Registry Expiry Date: 2024-07-14T15:28:43Z Registrar: NameCheap, Inc. Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: redemptionPeriod https://icann.org/epp#redemptionPeriod Name Server: DNS101.REGISTRAR-SERVERS.COM Name Server: DNS102.REGISTRAR-SERVERS.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2024-09-20T19:47:01Z <<<
WEBFIGMADESIGNERSHOP.COM	Domain name: WEBFIGMADESIGNERSHOP.COM Registry Domain ID: 2801604572_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-07-28T16:09:07.00Z Registrar Registration Expiration Date: 2024-07-28T16:09:07.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: pendingDelete https://icann.org/epp#pendingDelete Domain Status: redemptionPeriod https://icann.org/epp#redemptionPeriod Registry Registrant ID: Registrant Name: REACTIVATION PERIOD Registrant Organization: Withheld for Privacy Purposes

	Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: reactivation-pending@mail.withheldforprivacy.com Registry Admin ID: Admin Name: REACTIVATION PERIOD Admin Organization: Withheld for Privacy Purposes Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: reactivation-pending@mail.withheldforprivacy.com Registry Tech ID: Tech Name: REACTIVATION PERIOD Tech Organization: Withheld for Privacy Purposes Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: reactivation-pending@mail.withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-20T06:53:23.21Z <<<

WEBITRESOURSE.COM	Domain name: webitresourse.com Registry Domain ID: 2786631354_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-06-02T19:35:46.00Z Registrar Registration Expiration Date: 2024-06-02T19:35:46.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 042db3c6b292404b9120c05a47705b42.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext:

	Admin Email: 042db3c6b292404b9120c05a47705b42.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 042db3c6b292404b9120c05a47705b42.protect@withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ For more information on Whois status codes, please visit https://icann.org/epp
XACSHOP.COM	Domain Name: XACSHOP.COM Registry Domain ID: 2870474432_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.hostinger.com Registrar URL: http://www.hostinger.com Updated Date: 2024-04-08T13:50:55Z Creation Date: 2024-04-08T13:50:51Z Registry Expiry Date: 2025-04-08T13:50:51Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636 Registrar Abuse Contact Email: abuse-tracker@hostinger.com Registrar Abuse Contact Phone: +37064503378 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: NS1.DNS-PARKING.COM Name Server: NS2.DNS-PARKING.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

	>>> Last update of whois database: 2024-09-20T19:54:05Z <<<

.ORG REGISTRY
Public Interest Registry
11911 Freedom Drive, 10th Floor, Suite 1000
Reston, VA 20190

.ORG DOMAINS

EDITABLEZOOM.ORG	Domain Name: editablezoom.org Registry Domain ID: 40b4413522e74dc1ae89007355f64092-LROR Registrar WHOIS Server: https://rdapserver.net/ Registrar URL: http://www.hostinger.com Updated Date: 2024-03-20T13:34:36Z Creation Date: 2024-03-15T13:33:57Z Registry Expiry Date: 2025-03-15T13:33:57Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636 Registrar Abuse Contact Email: Registrar Abuse Contact Phone: Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: MA Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY

	Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of WHOIS database: 2024-09-20T19:56:16Z <<<
EICHENFASS.ORG	Domain Name: eichenfass.org Registry Domain ID: ecfc396b7971434c9970a1cdf34568ad-LROR Registrar WHOIS Server: https://rdapserver.net/ Registrar URL: http://www.hostinger.com Updated Date: 2024-07-13T16:19:35Z Creation Date: 2024-07-08T16:18:37Z Registry Expiry Date: 2025-07-08T16:18:37Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636 Registrar Abuse Contact Email: Registrar Abuse Contact Phone:

	Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: MA Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY

	Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of WHOIS database: 2024-09-20T19:56:51Z <<<
GOTHICSHOP.ORG	Domain Name: gothicshop.org Registry Domain ID: 29102a533cb94a9fb8c9dd5f9bd122e4-LROR Registrar WHOIS Server: https://rdapserver.net/ Registrar URL: http://www.hostinger.com Updated Date: 2024-05-12T13:14:54Z Creation Date: 2024-05-07T13:14:35Z Registry Expiry Date: 2025-05-07T13:14:35Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636 Registrar Abuse Contact Email: Registrar Abuse Contact Phone: Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: MA Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.

	Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of WHOIS database: 2024-09-20T19:57:35Z <<<
INVESTFIX.ORG	Domain Name: investfix.org Registry Domain ID: b2bfa484594b41ec91cd184c753d301d-LROR Registrar WHOIS Server: https://rdapserver.net/ Registrar URL: http://www.hostinger.com Updated Date: 2024-07-08T15:37:05Z Creation Date: 2024-07-03T15:36:27Z

	Registry Expiry Date: 2025-07-03T15:36:27Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636 Registrar Abuse Contact Email: Registrar Abuse Contact Phone: Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: MA Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY

	Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of WHOIS database: 2024-09-20T19:57:58Z <<<
LOYALTYFIRST.ORG	Domain Name: loyaltyfirst.org Registry Domain ID: 41b01ee0b0f44d80ac8c5eb249f3d7d6-LROR Registrar WHOIS Server: https://rdapserver.net/ Registrar URL: http://www.hostinger.com Updated Date: 2024-07-10T18:03:19Z Creation Date: 2024-07-05T18:02:58Z Registry Expiry Date: 2025-07-05T18:02:58Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636 Registrar Abuse Contact Email: Registrar Abuse Contact Phone: Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: MA Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY

	Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
MTGCGROUP.ORG	Domain Name: mtgcgroup.org

	Registry Domain ID: a0836b7399a443a58ef7b37113462d42-LROR Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2024-03-11T16:26:58Z Creation Date: 2024-03-06T16:26:32Z Registry Expiry Date: 2025-03-06T16:26:32Z Registrar: NameCheap, Inc. Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: Capital Region Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: IS Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.

	Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of WHOIS database: 2024-09-20T19:59:11Z <<<
MUTUALRESCUEBOOK.ORG	Domain Name: mutualrescuebook.org Registry Domain ID: ec34753585114c108fc4a7235a77ad00-LROR Registrar WHOIS Server: https://rdapserver.net/ Registrar URL: http://www.hostinger.com Updated Date: 2024-07-12T16:08:34Z Creation Date: 2024-05-19T12:01:07Z Registry Expiry Date: 2025-05-19T12:01:07Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636 Registrar Abuse Contact Email: Registrar Abuse Contact Phone: Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: MA Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US

	Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

	>>> Last update of WHOIS database: 2024-09-20T20:00:45Z <<<
MYGEIGER.ORG	Domain Name: mygeiger.org Registry Domain ID: b160a2dbb15a4f2bac6d38412760c675-LROR Registrar WHOIS Server: https://rdapserver.net/ Registrar URL: http://www.hostinger.com Updated Date: 2024-04-24T15:53:16Z Creation Date: 2024-04-19T15:53:10Z Registry Expiry Date: 2025-04-19T15:53:10Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636 Registrar Abuse Contact Email: Registrar Abuse Contact Phone: Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: MA Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY

	Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of WHOIS database: 2024-09-20T20:01:18Z <<<
PARTICLESOLID.ORG	Domain Name: particlesolid.org Registry Domain ID: c3e9dad867f74507b8bfd5e435089a6f-LROR Registrar WHOIS Server: https://rdapserver.net/ Registrar URL: http://www.hostinger.com Updated Date: 2024-04-29T09:48:58Z Creation Date: 2024-03-01T18:09:00Z Registry Expiry Date: 2025-03-01T18:09:00Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636 Registrar Abuse Contact Email: Registrar Abuse Contact Phone: Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: REDACTED FOR PRIVACY

	Registrant City: REDACTED FOR PRIVACY Registrant State/Province: MA Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: 123ns1.dns-parking.com Name Server: 123ns2.dns-parking.com

	DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of WHOIS database: 2024-09-20T20:02:01Z <<<
QUANTUMNYX.ORG	Domain Name: quantumnyx.org Registry Domain ID: 408f350f60f44bb6bc5fe23ba8878f84-LROR Registrar WHOIS Server: https://rdapserver.net/ Registrar URL: http://www.hostinger.com Updated Date: 2024-07-24T16:12:48Z Creation Date: 2024-07-19T16:12:16Z Registry Expiry Date: 2025-07-19T16:12:16Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636 Registrar Abuse Contact Email: Registrar Abuse Contact Phone: Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: MA Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY

	Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of WHOIS database: 2024-09-20T20:02:42Z <<<
YAMARU.ORG	Domain Name: yamaru.org Registry Domain ID: 208695d5b71e497d9409d71ae3409fc7-LROR Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2024-03-11T15:28:19Z Creation Date: 2024-03-06T15:27:54Z Registry Expiry Date: 2025-03-06T15:27:54Z Registrar: NameCheap, Inc. Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY

	Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: Capital Region Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: IS Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for

	information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of WHOIS database: 2024-09-20T20:03:34Z <<<

.NET REGISTRY
VeriSign Global Registry Services
12061 Bluemont Way
Reston VA 20190

.NET DOMAIN

DESGNSPIRATION.NET	Domain Name: DESGNSPIRATION.NET Registry Domain ID: 2862669470_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.PublicDomainRegistry.com Registrar URL: http://www.publicdomainregistry.com Updated Date: 2024-03-11T13:16:14Z Creation Date: 2024-03-11T13:16:14Z Registry Expiry Date: 2025-03-11T13:16:14Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Registrar Abuse Contact Email: Registrar Abuse Contact Phone: +1.2013775952 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: DNS1.REGWAY.COM Name Server: DNS2.REGWAY.COM Name Server: DNS3.REGWAY.COM Name Server: DNS4.REGWAY.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2024-09-20T20:08:43Z <<<
JUSTAPPLE.NET	Domain Name: justapple.net Registry Domain ID: 2867801843_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2024-03-29T15:49:10Z Creation Date: 2024-03-29T15:49:07Z Registry Expiry Date: 2025-03-29T15:49:07Z Registrar: NameCheap, Inc. Registrar IANA ID: 1068

	Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: DNS1.REGISTRAR-SERVERS.COM Name Server: DNS2.REGISTRAR-SERVERS.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2024-09-20T20:10:42Z <<<
OMMAHAT.NET	Domain name: ommahat.net Registry Domain ID: 2864908040_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2024-03-19T12:16:58.00Z Registrar Registration Expiration Date: 2025-03-19T12:16:58.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 2047e9ea4c3f42bab22af7c54e1a5295.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2

	Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 2047e9ea4c3f42bab22af7c54e1a5295.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 2047e9ea4c3f42bab22af7c54e1a5295.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-20T14:12:19.77Z <<<
CITYESSENTIALS.NET	Domain Name: CITYESSENTIALS.NET Registry Domain ID: 2882624142_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.hostinger.com Registrar URL: https://www.hostinger.com Updated Date: 2024-07-19T02:16:49Z Creation Date: 2024-05-19T15:30:15Z Registrar Registration Expiration Date: 2025-05-19T15:30:15Z Registrar: Hostinger Operations, UAB Registrar IANA ID: 1636 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry

	Registrant Name: Domain Admin Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: 10 Corporate Drive Registrant City: Burlington Registrant State/Province: MA Registrant Postal Code: 01803 Registrant Country: US Registrant Phone: +1.8022274003 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@privacyprotect.org Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: Privacy Protect, LLC (PrivacyProtect.org) Admin Street: 10 Corporate Drive Admin City: Burlington Admin State/Province: MA Admin Postal Code: 01803 Admin Country: US Admin Phone: +1.8022274003 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact@privacyprotect.org Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: Privacy Protect, LLC (PrivacyProtect.org) Tech Street: 10 Corporate Drive Tech City: Burlington Tech State/Province: MA Tech Postal Code: 01803 Tech Country: US Tech Phone: +1.8022274003 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@privacyprotect.org Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse@hostinger.com Registrar Abuse Contact Phone: +37064503378 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-20T20:13:44Z <<<

SGMODS.NET	Domain name: sgmods.net Registry Domain ID: 2875558934_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2024-04-25T14:39:04.00Z Registrar Registration Expiration Date: 2025-04-25T14:39:04.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: b8999297390441729eddc3a8cc2bf368.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext:

	Admin Email: b8999297390441729eddc3a8cc2bf368.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: b8999297390441729eddc3a8cc2bf368.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-20T19:15:52.11Z <<<

.ONLINE REGISTRY
Radix Technologies Inc.
Services Cayman Limited, P.O. Box 10008, Willow House, Cricket Square, Grand Cayman KY1-1001
Cayman Islands (the)

.ONLINE DOMAIN

PROTECTIONOFFICE.ONLINE	Domain Name: PROTECTIONOFFICE.ONLINE Registry Domain ID: D319531822-CNIC Registrar WHOIS Server: whois.hostinger.com Registrar URL: https://www.hostinger.com/ Updated Date: 2023-08-26T01:06:09.0Z Creation Date: 2022-08-25T07:55:24.0Z Registry Expiry Date: 2024-08-25T23:59:59.0Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

	Domain Status: autoRenewPeriod https://icann.org/epp#autoRenewPeriod Registrant Organization: Not Applicable Registrant State/Province: FL Registrant Country: US Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: DNS3.PARKPAGE.FOUNDATIONAPI.COM Name Server: DNS4.PARKPAGE.FOUNDATIONAPI.COM DNSSEC: unsigned Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registrar Abuse Contact Email: domains@hostinger.com Registrar Abuse Contact Phone: +370.68424669 URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

.TECH REGISTRY
Radix Technologies Inc.
Services Cayman Limited, P.O. Box 10008, Willow House, Cricket Square, Grand Cayman KY1-1001
Cayman Islands (the)

.TECH DOMAIN

PREVIEW-DOCUMENT.TECH	Domain Name: PREVIEW-DOCUMENT.TECH Registry Domain ID: D361616076-CNIC Registrar WHOIS Server: whois.hostinger.com Registrar URL: https://www.hostinger.com/ Updated Date: 2024-05-21T01:36:58.0Z Creation Date: 2023-04-14T12:54:16.0Z Registry Expiry Date: 2024-04-14T23:59:59.0Z Registrar: HOSTINGER operations, UAB

	Registrar IANA ID: 1636 Domain Status: pendingDelete https://icann.org/epp#pendingDelete Domain Status: serverHold https://icann.org/epp#serverHold Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: redemptionPeriod https://icann.org/epp#redemptionPeriod Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant State/Province: MA Registrant Country: US Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: NS1.DNS-EXPIRED.COM Name Server: NS2.DNS-EXPIRED.COM DNSSEC: unsigned Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registrar Abuse Contact Email: abuse@hostinger.com Registrar Abuse Contact Phone: +370.68424669 URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
PROTECTIONOFFICE.TECH	Domain Name: PROTECTIONOFFICE.TECH Registry Domain ID: D401427312-CNIC Registrar WHOIS Server: whois.hostinger.com Registrar URL: https://www.hostinger.com/ Updated Date: 2023-10-10T11:34:53.0Z Creation Date: 2023-10-05T11:33:46.0Z Registry Expiry Date: 2024-10-05T23:59:59.0Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636

	Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant State/Province: MA Registrant Country: US Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: NS2.PROTECTIONOFFICE.TECH Name Server: NS1.PROTECTIONOFFICE.TECH DNSSEC: unsigned Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registrar Abuse Contact Email: abuse@hostinger.com Registrar Abuse Contact Phone: +370.68424669 URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of WHOIS database: 2024-09-20T20:22:04.0Z <<<

EXHIBIT 2

Contents

1. Objective 1
2. Approach 2
3. Inputs 2
4. Outputs 8
5. References 11

WHOIS Proxy / Privacy Service Abuse Study – Draft Definition

This study will measure how often domains associated with illegal or harmful Internet communication abuse Privacy/Proxy services to obscure the perpetrator's identity.

Reviewer feedback is requested on study purpose, methodology, inputs, dependencies, outputs, and limitations – key discussion questions are highlighted by boxes like this one.

1. Objective

This study is intended to help the ICANN community determine the extent to which Proxy and Privacy services are abused during illegal or harmful Internet communication. Specifically, it will attempt to prove/disprove the following hypothesis:

> **A significant percentage of the domain names used to conduct illegal or harmful Internet activities are registered via Privacy or Proxy services to obscure the perpetrator's identity.**

As defined by [1], "illegal or harmful communication" refers to online activities (e.g., email messages, web transactions, file downloads) that violate criminal or civil law or which harm their targets (e.g., email/download recipients, website visitors). These activities include unsolicited commercial bulk email (spam), online intellectual property or identity theft, email harassment or stalking, phishing websites, online malware dissemination, and cybersquatting. Further examples include DoS attacks, DNS cache poisoning, pirated software (warez) distribution sites, money laundering email (mules scams), advanced fee fraud email (411 scams), and online sale of counterfeit merchandise or pharmaceuticals.

Allegations of actionable harm may require victims, law enforcement officials, and others to contact domain users (i.e., owners or licensees). To facilitate identification and contact, section 3.3.1 of the ICANN Registrar Accreditation Agreement (RAA) [4] requires Registrars to provide an interactive web page and a port 43 WHOIS service to enable free access to up-to-date data concerning all active registered domain names. This WHOIS data includes the name and postal address of the Registered Name Holder and technical and administrative contacts for the domain.

According to [1], Proxy and Privacy registration services provide anonymity or privacy protection for domain users. *Privacy* services hide certain user details from WHOIS by offering alternate contact information and mail forwarding services while not actually shielding the user's identity. *Proxy* services have a third-party register domain names on the user's behalf and then license the use of the domain name so that a third-party's contact information (and not the licensee's) is published in WHOIS. According to the WHOIS Privacy/Proxy Prevalence Study [3], approximately 15 to 25 percent of gTLD domain names are likely to be registered using a Privacy or Proxy service.

Study proposals [8][9][10] suggest that Privacy/Proxy services are being abused to obscure the identity of perpetrators that instigate illegal or harmful Internet communication, thereby impeding investigation. For example, proposal [8] indicates that Privacy/Proxy registrations lengthen phishing website take-down times. Proposal [9] indicates that Privacy/Proxy services are being abused to shield cyber squatters (i.e., parties that register or use a domain name in bad faith to profit from someone else's trademark).

A recent study of 384 domains hosted by ISP 3FN (shut down in June 2009 for abetting criminal activity) found that 38 percent were registered to Proxy services [11]. Of those, approximately half were associated with least one kind of illegal activity. Although small and informal, this study illustrated that domains used by criminals do use Proxy services – in this case, more often than the random domains studied by [3].

To provide the ICANN community with empirical data to evaluate such concerns, this study will methodically analyze a large, broad sample of domains associated with various kinds of illegal or harmful Internet activities. It will measure how often these alleged "bad actors" abuse Privacy/Proxy services, comparing rates for each kind of activity to overall Privacy/Proxy rates measured by [3]. If those rates are found to be significant, policy changes may be warranted to deter Privacy/Proxy abuse.

Note: This study will NOT measure the frequency of illegal/harmful Internet activity. This study will gather a representative sample of illegal/harmful incidents to measure how often Privacy/Proxy services are abused by perpetrators (alleged and confirmed).

2. Approach

This hypothesis will be tested by performing a descriptive study on a representative sample of domains within the top five gTLDs (.biz, .com, .info, .net, .org). To focus on study goals, this sample will be composed exclusively of domains involved in illegal or harmful Internet communication, as documented by organizations that routinely track, investigate, and/or remediate various kinds of activities. To measure frequency of abuse, this study will divvy sampled domain users into those that can be reached directly using WHOIS data and those that must be contacted via a referenced Privacy/Proxy service.

Because creating a single sample that proportionally represents every major kind of illegal or harmful Internet communication is unrealistic, subsamples will be created for each activity to be studied (e.g., a spam sender list, a warez site list). Many domains are

likely to be associated with multiple activities and may thus appear in more than one subsample. However, rates will be measured independently for each subsample to determine which activities most often abuse Privacy/Proxy services.

Furthermore, because the nature and duration of illegal/harmful Internet activities varies, different methods will be required for incident tracking, investigation, and remediation.

- Timely response is essential for extremely **short-lived activities** (e.g., spam, phishing, DoS attacks). Where possible, domain subsamples for these activities will be generated by monitoring **live-feeds** (e.g., real-time blacklists), letting researchers query and record WHOIS data in near-real-time.

- Timely response is less critical for activities associated with **long-lived activities** (e.g., trademark infringement, cybersquatting). Subsamples for these activities would be impossible to generate in near-real-time; live-feeds do not exist. Instead, these domains and WHOIS data will be **recorded over time** by study participants routinely involved in these incidents (e.g., first responders and real-time cybercrime researchers, complaint centers and law enforcement agencies, victim advocates).

To meet this study's goals, Privacy/Proxy determination must be based on WHOIS data as it was at the time of the incident. WHOIS queries usually return Registrant data long after an offending domain's web, file, or mail servers disappear, appear on an RBL, or are taken down. However, WHOIS data may well change following illegal activity, such as when a malicious domain is suspended or re-registered. Study goals can still be met so long as a significant percentage of WHOIS queries performed shortly after incidents do not return recently-updated or no Registrant data.

Note that other WHOIS studies [3][6][7] have been defined to measure the overall frequency of Privacy/Proxy use, what types of entities (e.g., natural or legal persons) commonly use Privacy/Proxy-registered domains and for what apparent purpose (e.g., personal or commercial), and how Privacy/Proxy providers respond to domain user reveal requests. Those questions are therefore outside the scope of this study.

However, overall frequency of Privacy/Proxy use [3] must be considered when sizing this study's subsamples so that they represent the top 5 gTLD domain population with a 95% confidence interval. Furthermore, because harmful/illegal Internet communication tends to originate from certain countries and regions, live-feeds and incident reports may be geographically skewed. To reflect world-wide experiences, subsamples must be generated from input sources with international scope – for example, global RBLs.

Finally, this study should build upon the foundation laid by the WHOIS Accuracy Study [2] and WHOIS Privacy/Proxy Prevalence Study [3] as follows.

- **Sample Cleaning and Coding:** WHOIS data for every domain name must include certain mandatory values (e.g., Registrant Name), but there is no RFC-standard record format or even a single global database from which WHOIS data can be

obtained. The Accuracy Study [2] developed a methodology for cleaning sampled domain WHOIS data to eliminate parsing errors, translate non-ASCII characters, map Registrants to country code/name, and sort the sample by Regional Internet Registry.

- **Registrant Type Classification:** Next, based on WHOIS Registrant Name and Organization values, the Accuracy Study assigned each sampled domain one of the following Apparent Registrant Types: name completely missing or patently false, a natural person, an organization with or without a person's name, a multiple domain name holder (ISP or reseller), or a potential Privacy/Proxy service provider. All potential Privacy/Proxy service providers were then either confirmed or reclassified.

Even though this study's sample design process and parameters differ, researchers are strongly encouraged to apply the same sample cleaning, coding, and classification process to reduce cost and promote consistency across all WHOIS studies. In particular, the Accuracy Study's methodology for confirming potential Privacy/Proxy use should be applied, as this is the key differentiator upon which this study's findings will be based.

3. Inputs

The first step in conducting this study will be to generate subsamples of domain names associated with each kind of illegal or harmful Internet communication to be measured. As noted in Section 2, because activity nature and duration varies, this study will employ two different research methods: Live-Feed Monitoring for incidents typically reported in real-time and Offline Third-Party Recording for all other kinds of incidents.

Method 1: Live-Feed Monitoring

Domain names associated with the following short-live illegal/harmful Internet activities should ideally be collected from live-feed sources. Possible sources are listed below; additional suggestions are welcome. Researchers are expected to refine and finalize this source list during the first phase of the study.

As alleged "bad actors" are identified from live-feeds, reverse DNS lookups and WHOIS queries will be performed in near-real-time[1] to record the Registrant' Name, Organization, and Address for domain names associated with each incident. Note that "associated domain name" depends upon the type of activity (e.g., spam sender, phishing website, malware server).

Note that, after incident investigation, many alleged bad actors do not end up being the real perpetrators. For example, many spam senders and phishing servers will be "bots" -- compromised hosts used by criminals without the Registrant's knowledge. Furthermore, domains may be added to RBLs based on complaints rather than verified incidents.

[1] Researchers will need to work around port 43 rate limits by pacing WHOIS queries, retrying failed queries, arranging for preferential access from a WHOIS query provider, or enlisting the help of a live-feed supplier that already has preferential access.

However, these "false positive" incident reports still require investigation; WHOIS Registrant data for those domains plays a role in enabling (or inhibiting) investigation. Therefore, this study must gather and analyze the WHOIS data associated with *all* alleged bad actors (proven or otherwise). To avoid skewing results, this study will *also* analyze refined samples that have been filtered to weed out low-probability cases – for example, eliminating domains associated with fewer than N reported incidents. Objective sample filtering methods should be defined by researchers at study start; suggestions are welcome.

Once sufficiently large subsamples have been collected for each activity, they will be cleaned, coded, and classified by Registrant Type as described in Section 2 for statistical analysis as described in Section 4.

- **Spam:** Live-feeds from several major real-time Domain Name System Blacklists (DNSBLs) could be used to generate a subsample of spam sender IP addresses/ranges and associated unique domain names. Possible sources include Spamhaus Blocklist, Mailshell Live-Feed, SURBL, URIBL, and SORBS DNSBL.

- **Phishing:** Several major Phishing website live-feeds could be used to generate a subsample of phishing URLs and the domain names that host them. Possible sources include OpenDNS PhishTank and Internet Identity RealPhish.

- **Malware:** A subsample of domains used to host and disseminate malware could be created from live-feeds maintained by major malware researchers and/or Internet security vendors. Possible sources include SRI Malware Threat Center, FireEye Malware Analysis & Exchange, and Malware Domains.

- **Denial-of-Service and DNS Cache Poisoning:** Input is requested on live-feed sources that could be used to generate subsamples of domains that send harmful messages during these time-sensitive attacks. Potential sources include the IMPACT Global Response Centre NEWS feed and FIRST-member incident response teams.

Method 2: Offline Third-Party Recording

Domain names associated with less time-critical illegal/harmful activities will be gathered from third-parties that routinely respond to or track such incidents in large volume and might be willing to assist by recording WHOIS data early in their investigation. Candidates include first responders and real-time cybercrime researchers, Internet crime complaint centers and law enforcement agencies, and victim advocates. Possible participants are listed below; additional suggestions are welcome. Researchers are expected to refine and finalize this participant list during the first phase of the study.

Consistency and accuracy of reported data is always a concern whenever numerous independent parties supply input for aggregate statistical analysis. To address this concern, researchers will develop a short, simple incident reporting form and process that participants can use to record the type of illegal/harmful activity, associated domain name, and WHOIS Registrant Name, Organization, and Address in a timely fashion. Here

again, note that "associated domain name" depends upon the type of activity (e.g., phishing website, warez server, money laundering email sender).

At study start, researchers will identify and invite representative sources to participate. All participants must agree to record and report all incidents encountered as part of their normal operation during a specified study period (e.g., 30 days). In particular, participants shall be asked to report all alleged perpetrators (proven or otherwise), and to indicate whether investigation confirmed or refuted their alleged involvement in the incident. This data collection approach makes it possible to study both the entire sample and a refined sample, filtered to focus on high-probability bad actors.

Although these longer-lived incidents may not be as time-sensitive as those monitored by live-feed, participants must still perform reverse DNS lookups and WHOIS queries on alleged perpetrator IP addresses and domain names as soon as possible after incidents are detected, not at the end of the study period.

A submission process will be designed to minimize participant effort while promoting consistent, accurate reporting. After a sufficiently large/broad set of third-party reports have been submitted, researchers will clean, code, and classify WHOIS data by Registrant Type as described in Section 2 for analysis as described in Section 4.

- **Phishing:** In proposal [8], the Anti Phishing Working Group (APWG) offered to supply a global list of phishing URLs, domains used to host them, and associated shutdown times. Due to the short duration of phishing sites, live-feed monitoring is preferable. However, analyzing this activity with both research methods might be useful to determine whether results differ significantly.

- **Cybersquatting:** Data on domains cited in alleged cybersquatting incidents might be gathered by organizations like the International Trademark Association (INTA). Approved dispute resolution service providers involved in ICANN's Uniform Domain-Name Dispute Resolution Policy (UDRP) are another possible source, although waiting until a dispute is filed to query WHOIS may be too much delay.

- **Intellectual property theft**: Data on domains cited in intellectual property theft complaints might be gathered by organizations like the UK Alliance Against IP Theft or the International Intellectual Property Rights (IPR) Advisory Program. However, data might be more readily available from groups that routinely record and investigate specific kinds of IP theft complaints, described below.

- **Media Piracy:** Data on domain names used by servers that illegally share copyrighted movies and music might be gathered by The International Federation of the Phonographic Industry (IFPI), the Motion Picture Association of America (MPAA), the Recording Industry Association of America (RIAA), and their international counterparts.

- **Software Piracy:** Data on domain names used by servers that illegally distribute copyrighted software might be gathered by major software vendors like Microsoft and Adobe or from an anti-piracy organization like the Business Software Alliance (BSA).

- **Trademark Infringement:** Data on domain names alleged to infringe upon registered trademarks might be gathered by an organization like the International Trademark Association (INTA) or commercial first-responders like Mark Monitor.

- **Counterfeit Merchandise:** Data on domains that send email advertising counterfeit merchandise and illegal pharmaceuticals might be gathered by an investigative agency like the US National Intellectual Property Rights Coordination Center Cyber Crimes Section (CCS). However, given that spam (one primary vector for online sale of counterfeit merchandise) can be studied more easily via live-feed, it might not be necessary to study this activity with method 2.

- **Money Laundering:** Data on domains that send recruiting email associated with fraudulent money laundering scams might be gathered by legitimate job recruitment websites like Monster and HotJobs or by an organization like BobBear that focuses specifically on tracking this type of illegal activity.

- **Advanced Fee Fraud:** Data on domains that send solicitation email associated with advanced fee fraud scams might be gathered by a tracking site like Artists Against 419 or bodies that handle Internet fraud complaints such as the FBI/NWCC Internet Crime Complaint Center (IC3) and its counterparts in other countries.

- **Identity Theft:** Data on domains that send bait email associated with online identity thefts might be gathered by the FBI/NWCC Internet Crime Complaint Center (IC3) or the US National Intellectual Property Rights Coordination Center Identity Fraud Initiative. However, major online identity theft vectors like phishing and malware can be studied more easily via live-feed monitoring; reliably correlating reported identity thefts to specific email messages and domains that caused them could be difficult.

- **Child Pornography:** Data on domain names of servers involved in online distribution of child pornography might be gathered by US National Intellectual Property Rights Coordination Center Cybercrimes Child Exploitation Section (CES) and Operation Predator. However, study [11] found it hard to obtain WHOIS data for child porn domains because, not only were sites taken down, but domain names were suspended.

- **Harassment or Stalking:** Input is requested on how to obtain a representative subsample of domain names that send online harassment and cyber-stalking email. Incidents are reported to local law enforcement agencies like FBI field offices. While HaltAbuse.org tracks statistics, based upon data supplied voluntarily by victims, many victims are reluctant to disclose these crimes. The highly personal nature of these activities could make it difficult to obtain a representative subsample.

- **Other Cybercrimes:** The FBI/NWCC Internet Crime Complaint Center (IC3) might also be able to supply data on perpetrator domains cited in complaints by victims of other cybercrimes, including online auction, investment fraud, and Internet extortion.

Because domain subsamples are likely to have some degree of cross-over, other readily-available online resources can be consulted to confirm and expand upon the kinds of illegal or harmful Internet communication associated with each domain. For example, in addition to RBLs, study [11] searched for domains using ReputationAuthority.org, Google Safe Browsing, McAfee SiteAdvisor, and Malware Domain List (either by searching a published list or by attempting to browse a website).

For each sampled domain, an **Apparent Registrant Type** must be assigned using the methodology defined by the WHOIS Accuracy Study [2], including confirmation of all domains potentially registered using Privacy/Proxy services. After this classification has been completed, the following input data will be available for each sampled domain:

Raw Data recorded by monitoring live-feed or reported by study participants

- Domain Name
- Registrant Name (may be a Privacy/Proxy service)
- Registrant Organization (may be a Privacy/Proxy service)
- Full WHOIS record for the domain
- Number of Illegal or Harmful Activity reported for this domain
- Kind(s) of Illegal or Harmful Activity reported for this domain
- Input Source(s) which supplied this domain name
- Incident Investigation Outcome (confirmed, refuted, in-progress/unknown)

Additional Data supplied by researchers

- Apparent Registrant Country Code/Name
- Apparent Registrant Type: missing/false, natural person, organization, multiple domain holder, or Privacy/Proxy service provider
- Additional Kind(s) of Illegal or Harmful Activity associated with this domain, as determined by searching RBLs and site reputation lists

1. *Suggest additional authoritative participants **with global scope**?*
2. *Will participants be willing (or able) to collect representative data?*
3. *Objective filtering methods or criteria to eliminate false positive reports?*
4. *Other concerns or issues regarding viability of proposed study methods?*

4. Outputs

This study will quantify the frequency of Privacy/Proxy use among domains allegedly involved in illegal or harmful communication, broken down by kind of activity. To deliver these empirical results, this study will examine the WHOIS Registrant data associated with each sampled domain as follows.

- During classification, some domains will be found to have missing, patently false, or otherwise unusable WHOIS Registrant data, thereby impeding perpetrator identification. These domains represent another method of WHOIS abuse which should be measured and included in study findings, but do not constitute Privacy/Proxy abuse.

- During classification, some domains will be found to have WHOIS Registrant data that explicitly identifies and supplies direct contact information for a natural person, an organization (with or without a person's name), or a multiple domain holder. These Registrants may or may not actually be responsible for the reported illegal or harmful communication. For example, many domain names will be mapped to spambot-compromised residential broadband hosts or trojan-hacked websites operated by legitimate businesses. However, for the purposes of this study, the users of these domains shall be considered readily-identifiable and directly-contactable using Registrant data returned from a simple WHOIS query.

- The rest of the sample will consist of domains that, following classification, have WHOIS Registrant data that identifies an apparent Privacy/Proxy provider. For the purposes of this study, all such domains will be considered to have abused a Privacy/Proxy service for the purpose of obscuring perpetrator identification. To determine significance, this abuse rate shall be compared to the overall rate of Privacy/Proxy use measured by [3] (15-25%).

For each kind of activity studied, the following measurements will be derived from the entire subsample of alleged bad actors (including bots and other false positives):

- Percentage of entire sample that could not be analyzed, categorized by reason (e.g., false/missing WHOIS, recently modified WHOIS, suspended domain)
- Percentage of entire sample with Registrant NOT obscured via Privacy/Proxy, distributed by gTLD/country
- Percentage of entire sample apparently registered via Privacy service, distributed by gTLD/country
- Percentage of entire sample apparently registered via Proxy service, distributed by gTLD/country

For each kind of activity studied, similar measurements will also be derived from a refined subsample, filtered to reduce false positives and focus on confirmed bad actors:

- Percentage of refined sample that could not be analyzed, categorized by reason
- Percentage of refined sample with Registrant NOT obscured via Privacy/Proxy, distributed by gTLD/country
- Percentage of refined sample apparently registered via Privacy service, distributed by gTLD/country
- Percentage of refined sample apparently registered via Proxy service, distributed by gTLD/country

Finally, these results will be aggregated and used to answer the following questions:

- Are Privacy services abused more/less often by bad actors (alleged or confirmed)?
- Are Proxy services abused more/less often by bad actors (alleged or confirmed)?
- Which illegal/harmful activities are most likely to abuse Privacy/Proxy services?
- Which illegal/harmful activities are least likely to abuse Privacy/Proxy services?
- Were there any kinds of illegal/harmful Internet communication for which Privacy/Proxy abuse could not be studied in a reliable way and why?

5. References

[1] Working Definitions for Key Terms that May be Used in Future WHOIS Studies, GNSO Drafting Team, 18 February 2009

[2] Proposed Design for a Study of the Accuracy of Whois Registrant Contact Information (6558,6636), NORC, June 3, 2009

[3] ICANN's Study on the Prevalence of Domain Names Registered using a Privacy or Proxy Service among the top 5 gTLDs, ICANN, September 28, 2009

[4] Registrar Accreditation Agreement (RAA), ICANN, 21 May 2009

[5] Terms of Reference for WHOIS Misuse Studies, ICANN, September 2009

[6] Terms of Reference for WHOIS Registrant Identification Studies, ICANN, Oct 2009

[7] Terms of Reference for WHOIS Privacy/Proxy Reveal Studies, ICANN, In Progress

[8] Study Suggestion Number 13b/c, Measure growth of proxy/privacy services vis-à-vis all registrations, Laura Mather

[9] Study Suggestion Number Study 17, Identify why proxy/privacy service users use those services, Claudio DiGangi

[10] GAC Data Set 11, What is the percentage of domain names registered using proxy or privacy services that have been associated with fraud or other illegal activity, GAC Recommendations for WHOIS Studies, 16 April 2008

[11] Private Domain Registrations: Examining the relationship between private domain registrations and malicious domains at 3FN, Piscitello, October 2009

EXHIBIT 3

Welcome to the new ICANN.org! Learn more, and send us your feedback. ✖ Dismiss

Translations Français Español العربية

Русский 中文 Log In Sign Up

Search ICANN.org

ICANN

GET STARTED NEWS & MEDIA POLICY PUBLIC COMMENT RESOURCES

COMMUNITY IANA STEWARDSHIP & ACCOUNTABILITY

Resources

- About ICANN
  - Learning
  - Participate
    - What ICANN Does
    - Effect on the Internet
    - What's Going On Now
    - How to Participate
    - Newcomers Program
    - Fellowships
  - President's Corner
  - ICANN

What Does ICANN Do?

This page is available in: العربية | Deutsch | English | Español | Français | Italiano | 日本語 | 한국어 | Português | Русский | 中文

To reach another person on the Internet you have to type an address into your computer - a name or a number. That address has to be unique so computers know where to find each other. ICANN coordinates these unique identifiers across the world. Without that coordination we wouldn't have one global Internet.

ICANN was formed in 1998. It is a not-for-profit partnership of people from all over the world dedicated to keeping the Internet secure, stable and interoperable. It promotes competition and develops policy on the Internet's unique identifiers.

ICANN doesn't control content on the Internet. It cannot stop spam and it doesn't deal with access to the Internet. But through its coordination role of the Internet's naming system, it does have an important impact on the expansion and evolution of the Internet.

What is the domain name system?

Management
Organization Chart
Staff
Careers
▸ In Focus
▸ For Journalists

▸ Board
▸ Accountability & Transparency
▸ Governance
▸ Groups
▸ Contractual Compliance
▸ Registrars
▸ Registries
Operational Metrics
▸ Identifier Systems Security, Stability and Resiliency (IS-SSR)
▸ ccTLDs
▸ Internationalized Domain Names
▸ Universal Acceptance Initiative

The domain name system, or DNS, is a system designed to make the Internet accessible to human beings. The main way computers that make up the Internet find one another is through a series of numbers, with each number (called an "IP address") correlating to a different device. However it is difficult for the human mind to remember long lists of numbers so the DNS uses letters rather than numbers, and then links a precise series of letters with a precise series of numbers.

The end result is that ICANN's website can be found at "icann.org" rather than "192.0.32.7" – which is how computers on the network know it. One advantage to this system – apart from making the network much easier to use for people – is that a particular domain name does not have to be tied to one particular computer because the link between a particular domain and a particular IP address can be changed quickly and easily. This change will then be recognised by the entire Internet within 48 hours thanks to the constantly updating DNS infrastructure. The result is an extremely flexible system.

A domain name itself comprises two elements: before and after "the dot". The part to the right of the dot, such as "com", "net", "org" and so on, is known as a "top-level domain" or TLD. One company in each case (called a registry), is in charge of all domains ending with that particular TLD and has access to a full list of domains directly under that name, as well as the IP addresses with which those names are associated. The part before the dot is the domain name that you register and which is then used to provide online systems such as websites, email and so on. These domains are sold by a large number of "registrars", free to charge whatever they wish, although in each case they pay a set per-domain fee to the particular registry under whose name the domain is being registered.

ICANN draws up contracts with each registry*. It also runs an accreditation system for registrars. It is these contracts that provide a consistent and stable environment for the domain name system, and hence the Internet.

In summary then, the DNS provides an addressing system for the Internet so people can find particular websites. It is also the basis for email and many other online uses.

- Policy
- Public Comment
- Contact
- Help

What does ICANN have to do with IP addresses?

ICANN plays a similar administrative role with the IP addresses used by computers as it does with the domain names used by humans. In the same way that you cannot have two domain names the same (otherwise you never know where you would end up), for the same reason it is also not possible for there to be two IP addresses the same.

Again, ICANN does not run the system, but it does help co-ordinate how IP addresses are supplied to avoid repetition or clashes. ICANN is also the central repository for IP addresses, from which ranges are supplied to regional registries who in turn distribute them to network providers.

What about root servers?

Root servers are a different case again. There are 13 root servers – or, more accurately, there are 13 IP addresses on the Internet where root servers can be found (the servers that have one of the 13 IP addresses can be in dozens of different physical locations). These servers all store a copy of the same file which acts as the main index to the Internet's address books. It lists an address for each top-level domain (.com, .de, etc) where that registry's own address book can be found.

In reality, the root servers are consulted fairly infrequently (considering the size of the Internet) because once computers on the network know the address of a particular top-level domain they retain it, checking back only occasionally to make sure the address hasn't changed. Nonetheless, the root servers remain vital for the Internet's smooth functioning.

The operators of the root servers remain largely autonomous, but at the same time work with one another and with ICANN to make sure the system stays up-to-date with the Internet's advances and changes.

What is ICANN's role?

As mentioned earlier, ICANN's role is to oversee the huge and complex interconnected network of unique identifiers that allow

computers on the Internet to find one another.

This is commonly termed "universal resolvability" and means that wherever you are on the network – and hence the world – that you receive the same predictable results when you access the network. Without this, you could end up with an Internet that worked entirely differently depending on your location on the globe.

How is ICANN structured?

ICANN is made up of a number of different groups, each of which represent a different interest on the Internet and all of which contribute to any final decisions that ICANN's makes.

There are three "supporting organisations" that represent:

- The organisations that deal with IP addresses
- The organisations that deal with domain names
- The managers of country code top-level domains (a special exception as explained at the bottom).

Then there are four "advisory committees" that provide ICANN with advice and recommendations. These represent:

- Governments and international treaty organisations
- Root server operators
- Those concerned with the Internet's security
- The "at large" community, meaning average Internet users.

And finally, there is a Technical Liaison Group, which works with the organisations that devise the basic protocols for Internet technologies.

ICANN's final decisions are made by a Board of Directors. The Board is made up of 21 members: 15 of which have voting rights and six are non-voting liaisons. The majority of the voting members (eight of them) are chosen by an independent Nominating Committee and the remainder are nominated members from supporting organisations.

ICANN then has a President and CEO who is also a Board member and who directs the work of ICANN staff, who are based across the globe and help co-ordinate, manage and finally implement all the different discussions and decisions made by the supporting organisations and advisory committees. An ICANN Ombudsman acts as an independent reviewer of the work of the ICANN staff and Board.

How does ICANN make decisions?

When it comes to making technical changes to the Internet, here is a simplified rundown of the process:

Any issue of concern or suggested changes to the existing network is typically raised within one of the supporting organisations (often following a report by one of the advisory committees), where it is discussed and a report produced which is then put out for public review. If the suggested changes impact on any other group within ICANN's system, that group also reviews the suggested changes and makes its views known. The result is then put out for public review a second time.

At the end of that process, the ICANN Board is provided with a report outlining all the previous discussions and with a list of recommendations. The Board then discusses the matter and either approves the changes, approves some and rejects others, rejects all of them, or sends the issue back down to one of the supporting organisations to review, often with an explanation as to what the problems are that need to be resolved before it can be approved.

The process is then rerun until all the different parts of ICANN can agree a compromise or the Board of Directors make a decision on a report it is presented with.

How is ICANN held accountable?

ICANN has external as well as internal accountabilities.

Externally, ICANN is an organisation incorporated under the law of the State of California in the United States. That means ICANN must abide by the laws of the United States and can be called to account by the judicial system i.e. ICANN can be taken to court.

ICANN is also a non-profit public benefit corporation and its directors are legally responsible for upholding their duties under corporation law.

Internally, ICANN is accountable to the community through:

- Its bylaws
- The representative composition of the ICANN Board from across the globe
- An independent Nominating Committee that selects a majority of the voting Board members
- Senior staff who must be elected annually by the Board
- Three different dispute resolution procedures (Board reconsideration committee; Independent Review Panel; Ombudsman)

The full range of ICANN's accountability and transparency frameworks and principles are available online.

---

* There is an important exception to this in the form of "country code top-level domains" (ccTLDs) such as .de for Germany or .uk for the United Kingdom. There are over 250 ccTLDs, some of which have a contract with ICANN; others of which have signed working agreements with ICANN; and some of which have yet to enter any formal agreement with ICANN. ICANN however does carry out what is known as the "IANA function" in which every ccTLD's main address is listed so the rest of the Internet can find it. ICANN is also in the position where it can add new TLDs to the wider system, as it did in 2000 and 2004 when seven and six new TLDs respectively were "added to the root".

RSS Feeds

Community Wiki

ICANN Blog

Who We Are
Get Started
Learning
Participate
Groups
Board
President's Corner
Staff
Careers
Newsletter

Contact Us
Offices
Customer Service
Security Team
PGP Keys
Certificate Authority
Registry Liaison
AOC Review
Organizational Reviews
Request a Speaker
For Journalists

Accountability & Transparency
Accountability Mechanisms
Independent Review Process
Request for Reconsideration
Ombudsman

Governance
Documents
Agreements
AOC Review
Annual Report
Financials
Document Disclosure
Planning
Dashboard
RFPs
Litigation
Correspondence

Help
Dispute Resolution
Domain Name Dispute Resolution
Name Collision
Registrar Problems
WHOIS

© 2014 Internet Corporation For Assigned Names and Numbers. Privacy Policy Terms of Service
Cookie Policy

EXHIBIT 4

2013 Registrar Accreditation Agreement

1. **Registrar Accreditation Agreement**
2. **Whois Accuracy Program Specification**
3. **Registration Data Directory Service (Whois) Specification**
4. **Consensus and Temporary Policy Specification**
5. **Specification on Privacy and Proxy Registrations**
6. **Data Retention Specification**
7. **Registrar Information Specification**
8. **Additional Registrar Operation Specification**
9. **Registrants' Benefits and Responsibilities**
10. **Logo License Specification**
11. **Compliance Certificate**
12. **Transition Addendum**

Approved by the ICANN Board on 27 June 2013

Registrar Accreditation Agreement

This REGISTRAR ACCREDITATION AGREEMENT (this "Agreement") is by and between the Internet Corporation for Assigned Names and Numbers, a California non-profit, public benefit corporation ("ICANN"), and [Registrar Name], a [Organization type and jurisdiction] ("Registrar"), and shall be deemed made on _____, at Los Angeles, California, USA.

1. DEFINITIONS. For purposes of this Agreement, the following definitions shall apply:

1.1 "Account Holder" means the person or entity that is paying for the Registered Name or otherwise controls the management of the registered name, when that person or entity is not the Registered Name Holder.

1.2 "Accredited" or "Accreditation" means to identify and set minimum standards for the performance of registration functions, to recognize persons or entities meeting those standards, and to enter into an accreditation agreement that sets forth the rules and procedures applicable to the provision of Registrar Services.

1.3 "Affiliate" means a person or entity that, directly or indirectly, through one or more intermediaries, Controls, is controlled by, or is under common control with, the person or entity specified.

1.4 "Affiliated Registrar" is another Accredited registrar that is an Affiliate of Registrar.

1.5 "Applicable Registrar Family" means, with respect to Affiliated Registrars, such Affiliated Registrar as a group.

1.6 "Consensus Policy" has the meaning set forth in the Consensus Policies and Temporary Policies Specification attached hereto.

1.7 "Control" (including the terms "controlled by" and "under common control with") means the possession, directly or indirectly, of the power to direct or cause the direction of the management or policies of a person or entity, whether through the ownership of securities, as trustee or executor, by serving as an employee or a

member of a board of directors or equivalent governing body, by contract, by credit arrangement or otherwise.

1.8 "DNS" refers to the Internet domain-name system.

1.9 The "Effective Date" is _____.

1.10 The "Expiration Date" is _____.

1.11 "gTLD" or "gTLDs" refers to the top-level domain(s) of the DNS delegated by ICANN pursuant to a registry agreement that is in full force and effect, other than any country code TLD (ccTLD) or internationalized domain name (IDN) country code TLD.

1.12 "gTLD Zone-File Data" means all data contained in a DNS zone file for the registry, or for any subdomain for which Registry Services are provided and that contains Registered Names, as provided to nameservers on the Internet.

1.13 "Illegal Activity" means conduct involving use of a Registered Name sponsored by Registrar that is prohibited by applicable law and/or exploitation of Registrar's domain name resolution or registration services in furtherance of conduct involving the use of a Registered Name sponsored by Registrar that is prohibited by applicable law.

1.14 "Personal Data" refers to data about any identified or identifiable natural person.

1.15 "Registered Name" refers to a domain name within the domain of a gTLD, whether consisting of two (2) or more (e.g., john.smith.name) levels, about which a gTLD Registry Operator (or an Affiliate or subcontractor thereof engaged in providing Registry Services) maintains data in a Registry Database, arranges for such maintenance, or derives revenue from such maintenance. A name in a Registry Database may be a Registered Name even though it does not appear in a zone file (e.g., a registered but inactive name).

1.16 "Registered Name Holder" means the holder of a Registered Name.

1.17 The word "registrar," when appearing without an initial capital letter, refers to a person or entity that contracts with Registered Name Holders and with a Registry Operator and collects registration data about the Registered Name Holders and submits registration information for entry in the Registry Database.

1.18 "Registrar Approval" means the receipt of either of the following approvals:

1.18.1 The affirmative approval of Applicable Registrars accounting for 90% of the Total Registered Names Under Management by the Applicable Registrars; provided that, for purposes of calculating the Total Registered

Names Under Management by Applicable Registrars, the Total Registered Names Under Management by each Applicable Registrar Family shall not exceed the Total Registered Names Under Management of the Applicable Registrar Family that is the fifth largest Applicable Registrar Family (measured by number of Registered Names Under Management), both for purposes of the numerator and the denominator; or

1.18.2 The affirmative approval of 50% plus one of the Applicable Registrars that participate in the process to approve or disapprove (i.e. vote for or against, but not abstain or otherwise fail to vote) a proposed amendment under Section 6, and the affirmative approval of Applicable Registrars accounting for 66.67% of the Total Registered Names Under Management by all Applicable Registrars; provided that, for purposes of calculating the Total Registered Names Under Management by Applicable Registrars, the Total Registered Names Under Management by each Applicable Registrar Family shall not exceed the total Registered Names Under Management of the Applicable Registrar Family that is the fifth largest Applicable Registrar Family (measured by number of Registered Names Under Management), both for purposes of the numerator and the denominator. An example of these calculations is set forth in Appendix 1 attached hereto.

1.19 "Registrar Services" means the services subject to this Agreement provided by a registrar in connection with a gTLD, and includes contracting with Registered Name Holders, collecting registration data about the Registered Name Holders, and submitting registration information for entry in the Registry Database.

1.20 "Registry Data" means all Registry Database data maintained in electronic form, and shall include gTLD Zone-File Data, all data used to provide Registry Services and submitted by registrars in electronic form, and all other data used to provide Registry Services concerning particular domain name registrations or nameservers maintained in electronic form in a Registry Database.

1.21 "Registry Database" means a database comprised of data about one or more DNS domain names within the domain of a registry that is used to generate either DNS resource records that are published authoritatively or responses to domain-name availability lookup requests or Whois queries, for some or all of those names.

1.22 A "Registry Operator" is the person or entity then responsible, in accordance with an agreement between ICANN (or its assignee) and that person or entity (those persons or entities) or, if that agreement is terminated or expires, in accordance with an agreement between the US Government and that person or entity (those persons or entities), for providing Registry Services for a specific gTLD.

1.23 "Registry Services," with respect to a particular gTLD, shall have the meaning defined in the agreement between ICANN and the Registry Operator for that gTLD.

1.24 A "Reseller" is a person or entity that participates in Registrar's distribution channel for domain name registrations (a) pursuant to an agreement, arrangement or understanding with Registrar or (b) with Registrar's actual knowledge, provides some or all Registrar Services, including collecting registration data about Registered Name Holders, submitting that data to Registrar, or facilitating the entry of the registration agreement between the Registrar and the Registered Name Holder.

1.25 "Restricted Amendment" means (i) an amendment of the Consensus Policies and Temporary Policies Specification or (ii) the term of this Agreement as specified in Section 5.1, as such term may be extended pursuant to Section 5.2.

1.26 A Registered Name is "sponsored" by the registrar that placed the record associated with that registration into the registry. Sponsorship of a registration may be changed at the express direction of the Registered Name Holder or, in the event a registrar loses Accreditation, in accordance with then-current ICANN Specifications and Policies.

1.27 "Specifications and/or Policies" include Consensus Policies, Specifications (such as the Whois Accuracy Program Specification) referenced in this Agreement, and any amendments, policies, procedures, or programs specifically contemplated by this Agreement or authorized by ICANN's Bylaws.

1.28 "Term of this Agreement" begins on the Effective Date and continues to the earlier of (a) the Expiration Date, or (b) termination of this Agreement.

1.29 "Total Registered Names Under Management" means the total number of Registered Names sponsored by all Applicable Registrars as reflected in the latest monthly reports submitted to ICANN by Registrars.

1.30 "Whois Accuracy Program Specification" means the Whois Accuracy Program Specification attached hereto, as updated from time to time in accordance with this Agreement.

1.31 "Whois Specification" means the Registration Data Directory Service (Whois) Specification attached hereto, as updated from time to time in accordance with this Agreement.

1.32 "Working Group" means representatives of the Applicable Registrars and other members of the community that the Registrar Stakeholder Group appoints, from time to time, to serve as a working group to consult on amendments to the Applicable Registrar Agreements (excluding bilateral amendments pursuant to Section 6.9).

2. ICANN OBLIGATIONS.

2.1 Accreditation. During the Term of this Agreement and subject to the terms and conditions of this Agreement, Registrar is hereby Accredited by ICANN to act as a registrar (including to insert and renew registration of Registered Names in the Registry Database) for gTLDs.

2.2 Registrar Use of ICANN Name, Website and Trademarks. ICANN hereby grants to Registrar a non-exclusive, worldwide, royalty-free license during the Term of this Agreement (a) to state that it is Accredited by ICANN as a registrar for gTLDs, and (b) to link to pages and documents within the ICANN website. Subject to the terms and conditions set forth in the Logo License Specification attached hereto, ICANN hereby grants to Registrar a non-exclusive, worldwide right and license to use the Trademarks (as defined in the Logo License Specification). No other use of ICANN's name, website or Trademarks is licensed hereby. This license may not be assigned or sublicensed by Registrar to any other party, including, without limitation, any Affiliate of Registrar or any Reseller.

2.3 General Obligations of ICANN. With respect to all matters that impact the rights, obligations, or role of Registrar, ICANN shall during the Term of this Agreement:

2.3.1 exercise its responsibilities in an open and transparent manner;

2.3.2 not unreasonably restrain competition and, to the extent feasible, promote and encourage robust competition;

2.3.3 not apply standards, policies, procedures or practices arbitrarily, unjustifiably, or inequitably and not single out Registrar for disparate treatment unless justified by substantial and reasonable cause; and

2.3.4 ensure, through its reconsideration and independent review policies, adequate appeal procedures for Registrar, to the extent it is adversely affected by ICANN standards, policies, procedures or practices.

2.4 Use of ICANN Accredited Registrars. In order to promote competition in the registration of domain names, and in recognition of the value that ICANN-Accredited registrars bring to the Internet community, ICANN has ordinarily required gTLD registries under contract with ICANN to use ICANN-Accredited registrars, and ICANN will during the course of this agreement abide by any ICANN adopted Specifications or Policies requiring the use of ICANN-Accredited registrars by gTLD registries.

3. REGISTRAR OBLIGATIONS.

3.1 Obligations to Provide Registrar Services. During the Term of this Agreement, Registrar agrees that it will operate as a registrar for one or more gTLDs in accordance with this Agreement.

3.2 Submission of Registered Name Holder Data to Registry. During the Term of this Agreement:

3.2.1 As part of its registration of Registered Names in a gTLD, Registrar shall submit to, or shall place in the Registry Database operated by, the Registry Operator for the gTLD the following data elements:

3.2.1.1 The name of the Registered Name being registered;

3.2.1.2 The IP addresses of the primary nameserver and secondary nameserver(s) for the Registered Name;

3.2.1.3 The corresponding names of those nameservers;

3.2.1.4 Unless automatically generated by the registry system, the identity of the Registrar;

3.2.1.5 Unless automatically generated by the registry system, the expiration date of the registration; and

3.2.1.6 Any other data the Registry Operator requires be submitted to it.

The agreement between the Registry Operator of a gTLD and Registrar may, if approved by ICANN in writing, state alternative required data elements applicable to that gTLD, in which event, the alternative required data elements shall replace and supersede Subsections 3.2.1.1 through 3.2.1.6 stated above for all purposes under this Agreement but only with respect to that particular gTLD. When seeking approval for alternative required data elements, the data elements set forth in Subsections 3.2.1.1 through 3.2.1.6 should be considered suggested minimum requirements.

3.2.2 Within seven (7) days after receiving any updates from the Registered Name Holder to the data elements listed in Subsections 3.2.1.2, 3.1.2.3, and 3.2.1.6 for any Registered Name that Registrar sponsors, Registrar shall submit the updated data elements to, or shall place those elements in the Registry Database operated by, the relevant Registry Operator.

3.2.3 In order to allow reconstitution of the Registry Database in the event of an otherwise unrecoverable technical failure or a change in the designated Registry Operator, within ten (10) days of any such request by ICANN,

Registrar shall submit an electronic database containing the data elements listed in Subsections 3.2.1.1 through 3.2.1.6 for all active records in the registry sponsored by Registrar, in a format specified by ICANN, to the Registry Operator for the appropriate gTLD.

3.3 Public Access to Data on Registered Names. During the Term of this Agreement:

3.3.1 At its expense, Registrar shall provide an interactive web page and, with respect to any gTLD operating a "thin" registry, a port 43 Whois service (each accessible via both IPv4 and IPv6) providing free public query-based access to up-to-date (i.e., updated at least daily) data concerning all active Registered Names sponsored by Registrar in any gTLD. Until otherwise specified by a Consensus Policy, such data shall consist of the following elements as contained in Registrar's database:

3.3.1.1 The name of the Registered Name;

3.3.1.2 The names of the primary nameserver and secondary nameserver(s) for the Registered Name;

3.3.1.3 The identity of Registrar (which may be provided through Registrar's website);

3.3.1.4 The original creation date of the registration;

3.3.1.5 The expiration date of the registration;

3.3.1.6 The name and postal address of the Registered Name Holder;

3.3.1.7 The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the technical contact for the Registered Name; and

3.3.1.8 The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the administrative contact for the Registered Name.

The agreement between the Registry Operator of a gTLD and Registrar may, if approved by ICANN in writing, state alternative required data elements applicable to that gTLD, in which event, the alternative required data elements shall replace and supersede Subsections 3.3.1.1 through 3.3.1.8 stated above for all purposes under this Agreement but only with respect to that particular gTLD.

3.3.2 Upon receiving any updates to the data elements listed in Subsections 3.3.1.2, 3.3.1.3, and 3.3.1.5 through 3.3.1.8 from the Registered Name Holder,

Registrar shall promptly update its database used to provide the public access described in Subsection 3.3.1.

3.3.3 Registrar may subcontract its obligation to provide the public access described in Subsection 3.3.1 and the updating described in Subsection 3.3.2, provided that Registrar shall remain fully responsible for the proper provision of the access and updating.

3.3.4 Registrar shall abide by any Consensus Policy that requires registrars to cooperatively implement a distributed capability that provides query-based Whois search functionality across all registrars. If the Whois service implemented by registrars does not in a reasonable time provide reasonably robust, reliable, and convenient access to accurate and up-to-date data, the Registrar shall abide by any Consensus Policy requiring Registrar, if reasonably determined by ICANN to be necessary (considering such possibilities as remedial action by specific registrars), to supply data from Registrar's database to facilitate the development of a centralized Whois database for the purpose of providing comprehensive Registrar Whois search capability.

3.3.5 In providing query-based public access to registration data as required by Subsections 3.3.1 and 3.3.4, Registrar shall not impose terms and conditions on use of the data provided, except as permitted by any Specification or Policy established by ICANN. Unless and until ICANN establishes a different Consensus Policy, Registrar shall permit use of data it provides in response to queries for any lawful purposes except to: (a) allow, enable, or otherwise support the transmission by e-mail, telephone, postal mail, facsimile or other means of mass unsolicited, commercial advertising or solicitations to entities other than the data recipient's own existing customers; or (b) enable high volume, automated, electronic processes that send queries or data to the systems of any Registry Operator or ICANN-Accredited registrar, except as reasonably necessary to register domain names or modify existing registrations.

3.3.6 In the event that ICANN determines, following analysis of economic data by an economist(s) retained by ICANN (which data has been made available to Registrar), that an individual or entity is able to exercise market power with respect to registrations or with respect to registration data used for development of value-added products and services by third parties, Registrar shall provide third-party bulk access to the data subject to public access under Subsection 3.3.1 under the following terms and conditions:

> 3.3.6.1 Registrar shall make a complete electronic copy of the data available at least one (1) time per week for download by third parties who have entered into a bulk access agreement with Registrar.

3.3.6.2 Registrar may charge an annual fee, not to exceed US$10,000, for such bulk access to the data.

3.3.6.3 Registrar's access agreement shall require the third party to agree not to use the data to allow, enable, or otherwise support any marketing activities, regardless of the medium used. Such media include but are not limited to e-mail, telephone, facsimile, postal mail, SMS, and wireless alerts.

3.3.6.4 Registrar's access agreement shall require the third party to agree not to use the data to enable high-volume, automated, electronic processes that send queries or data to the systems of any Registry Operator or ICANN-Accredited registrar, except as reasonably necessary to register domain names or modify existing registrations.

3.3.6.5 Registrar's access agreement must require the third party to agree not to sell or redistribute the data except insofar as it has been incorporated by the third party into a value-added product or service that does not permit the extraction of a substantial portion of the bulk data from the value-added product or service for use by other parties.

3.3.7 To comply with applicable statutes and regulations and for other reasons, ICANN may adopt a Consensus Policy establishing limits (a) on the Personal Data concerning Registered Names that Registrar may make available to the public through a public-access service described in this Subsection 3.3 and (b) on the manner in which Registrar may make such data available. Registrar shall comply with any such Consensus Policy.

3.3.8 Registrar shall meet or exceed the requirements set forth in the Whois Specification.

3.4 Retention of Registered Name Holder and Registration Data.

3.4.1 For each Registered Name sponsored by Registrar within a gTLD, Registrar shall collect and securely maintain, in its own electronic database, as updated from time to time:

3.4.1.1 the data specified in the Data Retention Specification attached hereto for the period specified therein;

3.4.1.2 The data elements listed in Subsections 3.3.1.1 through 3.3.1.8;

3.4.1.3 the name and (where available) postal address, e-mail address, voice telephone number, and fax number of the billing contact;

3.4.1.4 any other Registry Data that Registrar has submitted to the Registry Operator or placed in the Registry Database under Subsection 3.2; and

3.4.1.5 the name, postal address, e-mail address, and voice telephone number provided by the customer of any privacy service or licensee of any proxy registration service, in each case, offered or made available by Registrar or its Affiliates in connection with each registration. Effective on the date that ICANN fully implements a Proxy Accreditation Program established in accordance with Section 3.14, the obligations under this Section 3.4.1.5 will cease to apply as to any specific category of data (such as postal address) that is expressly required to be retained by another party in accordance with such Proxy Accreditation Program.

3.4.2 During the Term of this Agreement and for two (2) years thereafter, Registrar (itself or by its agent(s)) shall maintain the following records relating to its dealings with the Registry Operator(s) and Registered Name Holders:

3.4.2.1 In electronic form, the submission date and time, and the content, of all registration data (including updates) submitted in electronic form to the Registry Operator(s);

3.4.2.2 In electronic, paper, or microfilm form, all written communications constituting registration applications, confirmations, modifications, or terminations and related correspondence with Registered Name Holders, including registration contracts; and

3.4.2.3 In electronic form, records of the accounts of all Registered Name Holders with Registrar.

3.4.3 During the Term of this Agreement and for two (2) years thereafter, Registrar shall make the data, information and records specified in this Section 3.4 available for inspection and copying by ICANN upon reasonable notice. In addition, upon reasonable notice and request from ICANN, Registrar shall deliver copies of such data, information and records to ICANN in respect to limited transactions or circumstances that may be the subject of a compliance-related inquiry; provided, however, that such obligation shall not apply to requests for copies of the Registrar's entire database or transaction history. Such copies are to be provided at Registrar's expense. In responding to ICANN's request for delivery of electronic data, information and records, Registrar may submit such information in a format reasonably convenient to Registrar and acceptable to ICANN so as to minimize disruption to the Registrar's business. In the event Registrar believes that the provision of any such data, information or records to ICANN would

violate applicable law or any legal proceedings, ICANN and Registrar agree to discuss in good faith whether appropriate limitations, protections, or alternative solutions can be identified to allow the production of such data, information or records in complete or redacted form, as appropriate. ICANN shall not disclose the content of such data, information or records except as expressly required by applicable law, any legal proceeding or Specification or Policy.

3.4.4 Notwithstanding any other requirement in this Agreement or the Data Retention Specification, Registrar shall not be obligated to maintain records relating to a domain registration beginning on the date two (2) years following the domain registration's deletion or transfer away to a different registrar.

3.5 Rights in Data. Registrar disclaims all rights to exclusive ownership or use of the data elements listed in Subsections 3.2.1.1 through 3.2.1.3 for all Registered Names submitted by Registrar to the Registry Database for, or sponsored by Registrar in, each gTLD for which it is Accredited. Registrar does not disclaim rights in the data elements listed in Subsections 3.2.1.4 through 3.2.1.6 and Subsections 3.3.1.3 through 3.3.1.8 concerning active Registered Names sponsored by it in each gTLD for which it is Accredited, and agrees to grant non-exclusive, irrevocable, royalty-free licenses to make use of and disclose the data elements listed in Subsections 3.2.1.4 through 3.2.1.6 and 3.3.1.3 through 3.3.1.8 for the purpose of providing a service or services (such as a Whois service under Subsection 3.3.4) providing interactive, query-based public access. Upon a change in sponsorship from Registrar of any Registered Name in each gTLD for which it is Accredited, Registrar acknowledges that the registrar gaining sponsorship shall have the rights of an owner to the data elements listed in Subsections 3.2.1.4 through 3.2.1.6 and 3.3.1.3 through 3.3.1.8 concerning that Registered Name, with Registrar also retaining the rights of an owner in that data. Nothing in this Subsection prohibits Registrar from (1) restricting bulk public access to data elements in a manner consistent with this Agreement and any Specifications or Policies or (2) transferring rights it claims in data elements subject to the provisions of this Subsection 3.5.

3.6 Data Escrow. During the Term of this Agreement, on a schedule, under the terms, and in the format specified by ICANN, Registrar shall submit an electronic copy of the data described in Subsections 3.4.1.2 through 3.4.1.5 to ICANN or, at Registrar's election and at its expense, to a reputable escrow agent mutually approved by Registrar and ICANN, such approval also not to be unreasonably withheld by either party. The data shall be held under an agreement among Registrar, ICANN, and the escrow agent (if any) providing that (1) the data shall be received and held in escrow, with no use other than verification that the deposited data is complete, consistent, and in proper format, until released to ICANN; (2) the data shall be released from escrow upon expiration without renewal or termination of this Agreement; and (3) ICANN's rights under the escrow agreement shall be assigned with any assignment of this Agreement. The escrow shall provide that in

the event the escrow is released under this Subsection, ICANN (or its assignee) shall have a non-exclusive, irrevocable, royalty-free license to exercise (only for transitional purposes) or have exercised all rights necessary to provide Registrar Services.

3.7 Business Dealings, Including with Registered Name Holders.

3.7.1 In the event ICANN adopts a Specification or Policy that is supported by a consensus of ICANN-Accredited registrars as reflected in the Registrar Stakeholder Group (or any successor group), establishing or approving a Code of Conduct for ICANN-Accredited registrars, Registrar shall abide by that Code of Conduct.

3.7.2 Registrar shall abide by applicable laws and governmental regulations.

3.7.3 Registrar shall not represent to any actual or potential Registered Name Holder that Registrar enjoys access to a registry for which Registrar is Accredited that is superior to that of any other registrar Accredited for that registry.

3.7.4 Registrar shall not activate any Registered Name unless and until it is satisfied that it has received a reasonable assurance of payment of its registration fee. For this purpose, a charge to a credit card, general commercial terms extended to creditworthy customers, or other mechanism providing a similar level of assurance of payment shall be sufficient, provided that the obligation to pay becomes final and non-revocable by the Registered Name Holder upon activation of the registration.

3.7.5 At the conclusion of the registration period, failure by or on behalf of the Registered Name Holder to consent that the registration be renewed within the time specified in a second notice or reminder shall, in the absence of extenuating circumstances, result in cancellation of the registration by the end of the auto-renew grace period (although Registrar may choose to cancel the name earlier).

3.7.5.1 Extenuating circumstances are defined as: UDRP action, valid court order, failure of a Registrar's renewal process (which does not include failure of a registrant to respond), the domain name is used by a nameserver that provides DNS service to third-parties (additional time may be required to migrate the records managed by the nameserver), the registrant is subject to bankruptcy proceedings, payment dispute (where a registrant claims to have paid for a renewal, or a discrepancy in the amount paid), billing dispute (where a registrant disputes the amount on a bill), domain name subject to litigation in a court of competent jurisdiction, or other circumstance as approved specifically by ICANN.

3.7.5.2 Where Registrar chooses, under extenuating circumstances, to renew a domain name without the explicit consent of the registrant, the registrar must maintain a record of the extenuating circumstances associated with renewing that specific domain name for inspection by ICANN consistent with clauses 3.4.2 and 3.4.3 of this registrar accreditation agreement.

3.7.5.3 In the absence of extenuating circumstances (as defined in Section 3.7.5.1 above), a domain name must be deleted within 45 days of either the registrar or the registrant terminating a registration agreement.

3.7.5.4 Registrar shall provide notice to each new registrant describing the details of their deletion and auto-renewal policy including the expected time at which a non-renewed domain name would be deleted relative to the domain's expiration date, or a date range not to exceed ten (10) days in length. If a registrar makes any material changes to its deletion policy during the period of the registration agreement, it must make at least the same effort to inform the registrant of the changes as it would to inform the registrant of other material changes to the registration agreement (as defined in clause 3.7.7 of the registrars accreditation agreement).

3.7.5.5 If Registrar operates a website for domain name registration or renewal, details of Registrar's deletion and auto-renewal policies must be clearly displayed on the website.

3.7.5.6 If Registrar operates a website for domain registration or renewal, it should state, both at the time of registration and in a clear place on its website, any fee charged for the recovery of a domain name during the Redemption Grace Period.

3.7.5.7 In the event that a domain which is the subject of a UDRP dispute is deleted or expires during the course of the dispute, the complainant in the UDRP dispute will have the option to renew or restore the name under the same commercial terms as the registrant. If the complainant renews or restores the name, the name will be placed in Registrar HOLD and Registrar LOCK status, the WHOIS contact information for the registrant will be removed, and the WHOIS entry will indicate that the name is subject to dispute. If the complaint is terminated, or the UDRP dispute finds against the complainant, the name will be deleted within 45 days. The registrant retains the right under the existing redemption grace period provisions to recover the name at any time during the Redemption Grace Period, and retains the right to renew the name before it is deleted.

3.7.6 Registrar shall not insert or renew any Registered Name in any gTLD registry in a manner contrary to (i) any Consensus Policy stating a list or specification of excluded Registered Names that is in effect at the time of insertion or renewal, or (ii) any list of names to be reserved from registration as required by the specific Registry Operator for which the Registrar is providing Registrar Services.

3.7.7 Registrar shall require all Registered Name Holders to enter into an electronic or paper registration agreement with Registrar including at least the provisions set forth in Subsections 3.7.7.1 through 3.7.7.12, and which agreement shall otherwise set forth the terms and conditions applicable to the registration of a domain name sponsored by Registrar. The Registered Name Holder with whom Registrar enters into a registration agreement must be a person or legal entity other than the Registrar, provided that Registrar may be the Registered Name Holder for domains registered for the purpose of conducting its Registrar Services, in which case the Registrar shall submit to the provisions set forth in Subsections 3.7.7.1 through 3.7.7.12 and shall be responsible to ICANN for compliance with all obligations of the Registered Name Holder as set forth in this Agreement and Specifications and Policies. Registrar shall use commercially reasonable efforts to enforce compliance with the provisions of the registration agreement between Registrar and any Registered Name Holder that relate to implementing the requirements of Subsections 3.7.7.1 through 3.7.7.12 or any Consensus Policy.

3.7.7.1 The Registered Name Holder shall provide to Registrar accurate and reliable contact details and correct and update them within seven (7) days of any change during the term of the Registered Name registration, including: the full name, postal address, e-mail address, voice telephone number, and fax number if available of the Registered Name Holder; name of authorized person for contact purposes in the case of an Registered Name Holder that is an organization, association, or corporation; and the data elements listed in Subsections 3.3.1.2, 3.3.1.7 and 3.3.1.8.

3.7.7.2 A Registered Name Holder's willful provision of inaccurate or unreliable information, its willful failure to update information provided to Registrar within seven (7) days of any change, or its failure to respond for over fifteen (15) days to inquiries by Registrar concerning the accuracy of contact details associated with the Registered Name Holder's registration shall constitute a material breach of the Registered Name Holder-registrar contract and be a basis for suspension and/or cancellation of the Registered Name registration.

3.7.7.3 Any Registered Name Holder that intends to license use of a domain name to a third party is nonetheless the Registered Name

Holder of record and is responsible for providing its own full contact information and for providing and updating accurate technical and administrative contact information adequate to facilitate timely resolution of any problems that arise in connection with the Registered Name. A Registered Name Holder licensing use of a Registered Name according to this provision shall accept liability for harm caused by wrongful use of the Registered Name, unless it discloses the current contact information provided by the licensee and the identity of the licensee within seven (7) days to a party providing the Registered Name Holder reasonable evidence of actionable harm.

3.7.7.4 Registrar shall provide notice to each new or renewed Registered Name Holder stating:

3.7.7.4.1 The purposes for which any Personal Data collected from the applicant are intended;

3.7.7.4.2 The intended recipients or categories of recipients of the data (including the Registry Operator and others who will receive the data from Registry Operator);

3.7.7.4.3 Which data are obligatory and which data, if any, are voluntary; and

3.7.7.4.4 How the Registered Name Holder or data subject can access and, if necessary, rectify the data held about them.

3.7.7.5 The Registered Name Holder shall consent to the data processing referred to in Subsection 3.7.7.4.

3.7.7.6 The Registered Name Holder shall represent that notice has been provided equivalent to that described in Subsection 3.7.7.4 to any third-party individuals whose Personal Data are supplied to Registrar by the Registered Name Holder, and that the Registered Name Holder has obtained consent equivalent to that referred to in Subsection 3.7.7.5 of any such third-party individuals.

3.7.7.7 Registrar shall agree that it will not process the Personal Data collected from the Registered Name Holder in a way incompatible with the purposes and other limitations about which it has provided notice to the Registered Name Holder in accordance with Subsection 3.7.7.4 above.

3.7.7.8 Registrar shall agree that it will take reasonable precautions to protect Personal Data from loss, misuse, unauthorized access or disclosure, alteration, or destruction.

3.7.7.9 The Registered Name Holder shall represent that, to the best of the Registered Name Holder's knowledge and belief, neither the registration of the Registered Name nor the manner in which it is directly or indirectly used infringes the legal rights of any third party.

3.7.7.10 For the adjudication of disputes concerning or arising from use of the Registered Name, the Registered Name Holder shall submit, without prejudice to other potentially applicable jurisdictions, to the jurisdiction of the courts (1) of the Registered Name Holder's domicile and (2) where Registrar is located.

3.7.7.11 The Registered Name Holder shall agree that its registration of the Registered Name shall be subject to suspension, cancellation, or transfer pursuant to any Specification or Policy, or pursuant to any registrar or registry procedure not inconsistent with any Specification or Policy, (1) to correct mistakes by Registrar or the Registry Operator in registering the name or (2) for the resolution of disputes concerning the Registered Name.

3.7.7.12 The Registered Name Holder shall indemnify and hold harmless the Registry Operator and its directors, officers, employees, and agents from and against any and all claims, damages, liabilities, costs, and expenses (including reasonable legal fees and expenses) arising out of or related to the Registered Name Holder's domain name registration.

3.7.8 Registrar shall comply with the obligations specified in the Whois Accuracy Program Specification. In addition, notwithstanding anything in the Whois Accuracy Program Specification to the contrary, Registrar shall abide by any Consensus Policy requiring reasonable and commercially practicable (a) verification, at the time of registration, of contact information associated with a Registered Name sponsored by Registrar or (b) periodic re-verification of such information. Registrar shall, upon notification by any person of an inaccuracy in the contact information associated with a Registered Name sponsored by Registrar, take reasonable steps to investigate that claimed inaccuracy. In the event Registrar learns of inaccurate contact information associated with a Registered Name it sponsors, it shall take reasonable steps to correct that inaccuracy.

3.7.9 Registrar shall abide by any Consensus Policy prohibiting or restricting warehousing of or speculation in domain names by registrars.

3.7.10 Registrar shall publish on its website(s) and/or provide a link to the Registrants' Benefits and Responsibilities Specification attached hereto and shall not take any action inconsistent with the corresponding provisions of this Agreement or applicable law.

3.7.11 Registrar shall make available a description of the customer service handling processes available to Registered Name Holders regarding Registrar Services, including a description of the processes for submitting complaints and resolving disputes regarding the Registrar Services.

3.7.12 Nothing in this Agreement prescribes or limits the amount Registrar may charge Registered Name Holders for registration of Registered Names.

3.8 Domain-Name Dispute Resolution. During the Term of this Agreement, Registrar shall have in place a policy and procedures for resolution of disputes concerning Registered Names. Until ICANN adopts an alternative Consensus Policy or other Specification or Policy with respect to the resolution of disputes concerning Registered Names, Registrar shall comply with the Uniform Domain Name Dispute Resolution Policy ("UDRP") identified on ICANN's website (www.icann.org/general/consensus-policies.htm), as may be modified from time to time. Registrar shall also comply with the Uniform Rapid Suspension ("URS") procedure or its replacement, as well as with any other applicable dispute resolution procedure as required by a Registry Operator for which Registrar is providing Registrar Services.

3.9 Accreditation Fees. As a condition of Accreditation, Registrar shall pay Accreditation fees to ICANN. These fees consist of yearly and variable fees.

3.9.1 Registrar shall pay ICANN a yearly Accreditation fee in an amount established by the ICANN Board of Directors, in conformity with ICANN's bylaws and articles of incorporation. This yearly Accreditation fee shall not exceed US$4,000. Payment of the yearly fee shall be due within thirty (30) days after invoice from ICANN, provided that Registrar may elect to pay the yearly fee in four (4) equal quarterly installments.

3.9.2 Registrar shall pay the variable Accreditation fees established by the ICANN Board of Directors, in conformity with ICANN's bylaws and articles of incorporation, provided that in each case such fees are reasonably allocated among all registrars that contract with ICANN and that any such fees must be expressly approved by registrars accounting, in the aggregate, for payment of two-thirds of all registrar-level fees. Registrar shall pay such fees in a timely manner for so long as all material terms of this Agreement remain in full force and effect, and notwithstanding the pendency of any dispute between Registrar and ICANN.

3.9.3 For any payments thirty (30) days or more overdue, Registrar shall pay interest on late payments at the rate of 1.5% per month or, if less, the maximum rate permitted by applicable law from later of the date of the invoice or the date the invoice is sent pursuant to Section 7.6 of this Agreement. On reasonable notice given by ICANN to Registrar, accountings submitted by Registrar shall be subject to verification by an audit of

Registrar's books and records by an independent third-party designated by ICANN that shall preserve the confidentiality of such books and records (other than its findings as to the accuracy of, and any necessary corrections to, the accountings).

3.9.4 The Accreditation fees due under this Agreement are exclusive of tax. All taxes, duties, fees and other governmental charges of any kind (including sales, turnover, services, use and value-added taxes) that are imposed by or under the authority of any government or any political subdivision thereof on the Accreditation fees for any services, software and/or hardware shall be borne by Registrar and shall not be considered a part of, a deduction from, or an offset against such Accreditation fees. All payments due to ICANN shall be made without any deduction or withholding on account of any tax, duty, charge, or penalty except as required by applicable law, in which case, the sum payable by Registrar from which such deduction or withholding is to be made shall be increased to the extent necessary to ensure that, after making such deduction or withholding, ICANN receives (free from any liability with respect thereof) a net sum equal to the sum it would have received but for such deduction or withholding being required.

3.10 Insurance. Registrar shall maintain in force commercial general liability insurance or similar liability insurance as specified by ICANN with policy limits of at least US$500,000 covering liabilities arising from Registrar's registrar business during the Term of this Agreement.

3.11 Obligations of Registrars under common controlling interest. Registrar shall be in breach of this Agreement if:

3.11.1 ICANN terminates an Affiliated Registrar's accreditation agreement with ICANN (an "Affiliate Termination");

3.11.2 Affiliated Registrar has not initiated arbitration challenging ICANN's right to terminate the Affiliated Registrar's accreditation agreement under Section 5.8 of this Agreement, or has initiated such arbitration and has not prevailed;

3.11.3 the Affiliate Termination was the result of misconduct that materially harmed consumers or the public interest;

3.11.4 a second Affiliated Registrar has pursued, after the Affiliate Termination, the same course of conduct that resulted in the Affiliate Termination; and

3.11.5 ICANN has provided Registrar with written notice that it intends to assert the provisions of this Section 3.11 with respect to Registrar, which notice shall identify in reasonable detail the factual basis for such assertion,

and Registrar has failed to cure the impugned conduct within fifteen (15) days of such notice.

3.12 Obligations Related to Provision of Registrar Services by Third Parties. Registrar is responsible for the provision of Registrar Services for all Registered Names that Registrar sponsors being performed in compliance with this Agreement, regardless of whether the Registrar Services are provided by Registrar or a third party, including a Reseller. Registrar must enter into written agreements with all of its Resellers that enable Registrar to comply with and perform all of its obligations under this Agreement. In addition, Registrar must ensure that:

3.12.1 Its Resellers do not display the ICANN or ICANN-Accredited Registrar logo, or otherwise represent themselves as Accredited by ICANN, unless they have written permission from ICANN to do so.

3.12.2 Any registration agreement used by reseller shall include all registration agreement provisions and notices required by the ICANN Registrar Accreditation Agreement and any ICANN Consensus Policies, and shall identify the sponsoring registrar or provide a means for identifying the sponsoring registrar, such as a link to the InterNIC Whois lookup service.

3.12.3 Its Resellers identify the sponsoring registrar upon inquiry from the customer.

3.12.4 Its Resellers comply with any ICANN-adopted Specification or Policy that establishes a program for accreditation of individuals or entities who provide proxy and privacy registration services (a "Proxy Accreditation Program"). Among other features, the Proxy Accreditation Program may require that: (i) proxy and privacy registration services may only be provided in respect of domain name registrations by individuals or entities Accredited by ICANN pursuant to such Proxy Accreditation Program; and (ii) Registrar shall prohibit Resellers from knowingly accepting registrations from any provider of proxy and privacy registration services that is not Accredited by ICANN pursuant the Proxy Accreditation Program. Until such time as the Proxy Accreditation Program is established, Registrar shall require Resellers to comply with the Specification on Privacy and Proxy Registrations attached hereto.

3.12.5 Its Resellers' customers are provided with a link to an ICANN webpage detailing registrant educational information, as detailed in subsection 3.16 below.

3.12.6 In the event Registrar learns that a Reseller is causing Registrar to be in breach of any of the provisions of this Agreement, Registrar shall take reasonable steps to enforce its agreement with such Reseller so as to cure and prevent further instances of non-compliance.

3.12.7 Its Resellers shall publish on their website(s) and/or provide a link to the Registrants' Benefits and Responsibilities Specification attached hereto and shall not take any action inconsistent with the corresponding provisions of this Agreement or applicable law.

Registrar shall use commercially reasonable efforts to enforce compliance with the provisions of the agreement between Registrar and any Reseller that relate to the provisions of Registrar Services.

3.13 Registrar Training. Registrar's primary contact as identified in Subsection 7.6 below or designee (so long as the designee is employed by Registrar or an Affiliated Registrar) shall complete a training course covering registrar obligations under ICANN policies and agreements. The course will be provided by ICANN at no expense to Registrar, and shall be available in an online format.

3.14 Obligations Related to Proxy and Privacy Services. Registrar agrees to comply with any ICANN-adopted Specification or Policy that establishes a Proxy Accreditation Program. Registrar also agrees to reasonably cooperate with ICANN in the development of such program. Until such time as the Proxy Accreditation Program is established, Registrar agrees to comply with the Specification on Privacy and Proxy Registrations attached hereto.

3.15 Registrar Self-Assessment and Audits. Registrar shall complete and deliver to ICANN on a schedule and in the form specified by ICANN from time to time in consultation with registrars a Registrar self-assessment. Registrar shall complete and deliver to ICANN within twenty (20) days following the end of each calendar year, in a form specified by ICANN a certificate executed by the president, chief executive officer, chief financial officer or chief operating officer (or their equivalents) of Registrar certifying compliance with the terms and conditions of this Agreement. ICANN may from time to time (not to exceed twice per calendar year) conduct, or engage a third party to conduct on its behalf, contractual compliance audits to assess compliance by Registrar with the terms and conditions of this Agreement. Any audits pursuant to this Section 3.15 shall be tailored to achieve the purpose of assessing compliance, and ICANN will (a) give reasonable advance notice of any such audit, which notice shall specify in reasonable detail the categories of documents, data and other information requested by ICANN, and (b) use commercially reasonable efforts to conduct such audit in such a manner as to not unreasonably disrupt the operations of Registrar. As part of such audit and upon request by ICANN, Registrar shall timely provide all responsive documents, data and any other information necessary to demonstrate Registrar's compliance with this Agreement. Upon no less than ten (10) days notice (unless otherwise agreed to by Registrar), ICANN may, as part of any contractual compliance audit, conduct site visits during regular business hours to assess compliance by Registrar with the terms and conditions of this Agreement. ICANN shall not disclose Registrar confidential information gathered through such audits except as required by applicable law, legal proceedings, or as expressly permitted by any Specification or

Policy (including ICANN's Documentary Information Disclosure Policy, as such policy may be amended from time to time); provided, however, that, except as required by applicable law or legal proceedings, ICANN shall not release any information that Registrar has marked as, or has otherwise designated in writing to ICANN as, a "confidential trade secret," "confidential commercial information" or "confidential financial information" of Registrar. If any applicable law, legal proceeding or Specification or Policy permits such disclosure, ICANN will provide Registrar no less than fifteen (15) days notice of its intent to disclose such information, unless such notice is prohibited by law or legal proceeding. Such notice shall include to whom and in what manner ICANN plans to disclose such information.

3.16 Link to Registrant Educational Information. ICANN has published an educational webpage summarizing the terms of the Registrar Accreditation Agreement and related Consensus Policies (as of the date of this Agreement, located at: http://www.icann.org/en/registrars/registrant-rights-responsibilities-en.htm). Registrar shall provide a link to such webpage on any website it may operate for domain name registration or renewal clearly displayed to its Registered Name Holders at least as clearly as its links to policies or notifications required to be displayed under ICANN Consensus Policies. ICANN may, in consultation with registrars, update the content and/or URL for this website.

3.17 Registrar Contact, Business Organization and Officer Information. Registrar shall provide to ICANN and maintain accurate and current information as specified in the Registrar Information Specification to this Agreement. In addition, Registrar shall publish on each website through which Registrar provides or offers Registrar Services the information specified as requiring such publication in the Registrar Information Specification. Registrar shall notify ICANN within five (5) days of any changes to such information and update Registrar's website(s) within twenty (20) days of any such changes.

3.18 Registrar's Abuse Contact and Duty to Investigate Reports of Abuse.

3.18.1 Registrar shall maintain an abuse contact to receive reports of abuse involving Registered Names sponsored by Registrar, including reports of Illegal Activity. Registrar shall publish an email address to receive such reports on the home page of Registrar's website (or in another standardized place that may be designated by ICANN from time to time). Registrar shall take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse.

3.18.2 Registrar shall establish and maintain a dedicated abuse point of contact, including a dedicated email address and telephone number that is monitored 24 hours a day, seven days a week, to receive reports of Illegal Activity by law enforcement, consumer protection, quasi-governmental or other similar authorities designated from time to time by the national or

territorial government of the jurisdiction in which the Registrar is established or maintains a physical office. Well-founded reports of Illegal Activity submitted to these contacts must be reviewed within 24 hours by an individual who is empowered by Registrar to take necessary and appropriate actions in response to the report. In responding to any such reports, Registrar will not be required to take any action in contravention of applicable law.

3.18.3 Registrar shall publish on its website a description of its procedures for the receipt, handling, and tracking of abuse reports. Registrar shall document its receipt of and response to all such reports. Registrar shall maintain the records related to such reports for the shorter of two (2) years or the longest period permitted by applicable law, and during such period, shall provide such records to ICANN upon reasonable notice.

3.19 Additional Technical Specifications to Implement IPV6, DNSSEC and IDNs. Registrar shall comply with the Additional Registrar Operations Specification attached hereto.

3.20 Notice of Bankruptcy, Convictions and Security Breaches. Registrar will give ICANN notice within seven (7) days of (i) the commencement of any of the proceedings referenced in Section 5.5.8. (ii) the occurrence of any of the matters specified in Section 5.5.2 or Section 5.5.3 or (iii) any unauthorized access to or disclosure of registrant account information or registration data. The notice required pursuant to Subsection (iii) shall include a detailed description of the type of unauthorized access, how it occurred, the number of registrants affected, and any action taken by Registrar in response.

3.21 Obligations of Registrars Affiliated with Registry Operators. In the event Registrar is Affiliated with any Registry Operator or back-end registry operator (an "Affiliated Relationship") during the Term of this Agreement, Registrar shall comply with all ICANN Specifications and Policies that may be developed from time to time with respect to such Affiliated Relationships, and will notify ICANN within thirty (30) days of the occurrence of the event that created the Affiliate relationship (e.g., the closing of any merger, acquisition or other transaction, or the execution of any agreement, in each case, giving rise to such Affiliated Relationship).

3.22 Cooperation with Emergency Registry Service Providers. In the event that ICANN transitions the operation of a registry for a gTLD in which Registrar sponsors Registered Names to an emergency registry service provider, Registrar shall cooperate in all reasonable respects with such emergency registry service provider, including by entering into a registry-registrar agreement with such provider necessary to effect the transition and by providing all Registered Name Holder data reasonably requested by such emergency operator for the purpose of facilitating an efficient transition of the registry for the gTLD.

4. PROCEDURES FOR ESTABLISHMENT OR REVISION OF SPECIFICATIONS AND POLICIES.

4.1 Compliance with Consensus Policies and Temporary Policies. During the Term of this Agreement, Registrar shall comply with and implement all Consensus Policies and Temporary Policies in existence as of the Effective Date found at http://www.icann.org/general/consensus-policies.htm, and as may in the future be developed and adopted in accordance with the ICANN Bylaws, provided such future Consensus Policies and Temporary Policies are adopted in accordance with the procedures and relate to those topics and subject to those limitations set forth in the Consensus Policies and Temporary Policies Specification to this Agreement.

5. TERM, TERMINATION AND DISPUTE RESOLUTION.

5.1 Term of Agreement. This Agreement shall be effective on the Effective Date and shall have an initial term running until the Expiration Date, unless sooner terminated.

5.2 Renewal. This Agreement and Registrar's Accreditation will be renewed for successive periods of five (5) years upon the Expiration Date and the expiration of each successive five-year term thereafter under the terms and conditions of this Agreement, unless:

5.2.1 at the time of such renewal, Registrar no longer meets the ICANN registrar Accreditation criteria then in effect;

5.2.2 Registrar is not in compliance with its obligations under this Agreement at the time of the Expiration Date or at the expiration of any successive five (5) year term thereafter;

5.2.3 Registrar has been given notice by ICANN of three (3) or more material breaches of this Agreement within the two (2) years preceding the Expiration Date or the date of expiration of any successive five (5) year term thereafter; or

5.2.4 this Agreement has terminated prior to the Expiration Date or the expiration date of any successive five (5) year term thereafter.

In the event Registrar intends to renew this Agreement pursuant to this Section 5.2, Registrar shall provide ICANN written notice thereof during the period that is no more than ninety (90) days and no less than sixty (60) days prior to the Expiration Date and each successive five (5) year term thereafter. The provision of such notice shall not be a condition to renewal hereunder. Pursuant to its customary practices (as may be modified by ICANN), ICANN will provide notice to Registrar of the Expiration Date and the date of expiration of any subsequent term hereunder.

5.3 Right to Substitute Updated Agreement. In the event that, during the Term of this Agreement, ICANN adopts a revised form Registrar accreditation agreement (the "Updated RAA"), Registrar (provided it has not received (i) a notice of breach that it has not cured or (ii) a notice of termination or suspension of this Agreement under this Section 5) may elect, by giving ICANN written notice, to enter into the Updated RAA. In the event of such election, Registrar and ICANN shall as soon as practicable enter into the Updated RAA for the term specified in the Updated RAA, and this Agreement will be deemed terminated.

5.4 Termination of Agreement by Registrar. This Agreement may be terminated before its expiration by Registrar by giving ICANN thirty (30) days written notice. Upon such termination by Registrar, Registrar shall not be entitled to any refund of fees paid to ICANN pursuant to this Agreement.

5.5 Termination of Agreement by ICANN. This Agreement may be terminated before its expiration by ICANN in any of the following circumstances:

5.5.1 There was a material misrepresentation, material inaccuracy, or materially misleading statement in Registrar's application for Accreditation or renewal of Accreditation or any material accompanying the application.

5.5.2 Registrar:

5.5.2.1 is convicted by a court of competent jurisdiction of a felony or other serious offense related to financial activities, or is judged by a court of competent jurisdiction to have:

5.5.2.1.1 committed fraud,

5.5.2.1.2 committed a breach of fiduciary duty, or

5.5.2.1.3 with actual knowledge (or through gross negligence) permitted Illegal Activity in the registration or use of domain names or in the provision to Registrar by any Registered Name Holder of inaccurate Whois information; or

5.5.2.1.4 failed to comply with the terms of an order issued by a court of competent jurisdiction relating to the use of domain names sponsored by the Registrar;

or is the subject of a judicial determination that ICANN reasonably deems as the substantive equivalent of any of the foregoing; or

5.5.2.2 is disciplined by the government of its domicile for conduct involving dishonesty or misuse of funds of others; or

5.5.2.3 is the subject of a non-interlocutory order issued by a court or arbitral tribunal, in each case of competent jurisdiction, finding that Registrar has, directly or through an Affiliate, committed a specific violation(s) of applicable national law or governmental regulation relating to cybersquatting or its equivalent; or

5.5.2.4 is found by ICANN, based on its review of the findings of arbitral tribunals, to have been engaged, either directly or through its Affiliate, in a pattern and practice of trafficking in or use of domain names identical or confusingly similar to a trademark or service mark of a third party in which the Registered Name Holder has no rights or legitimate interest, which trademarks have been registered and are being used in bad faith.

5.5.3 Registrar knowingly employs any officer that is convicted of a misdemeanor related to financial activities or of any felony, or is judged by a court of competent jurisdiction to have committed fraud or breach of fiduciary duty, or is the subject of a judicial determination that ICANN reasonably deems as the substantive equivalent of any of the foregoing and such officer is not terminated within thirty (30) days of Registrar's knowledge of the foregoing; or any member of Registrar's board of directors or similar governing body is convicted of a misdemeanor related to financial activities or of any felony, or is judged by a court of competent jurisdiction to have committed fraud or breach of fiduciary duty, or is the subject of a judicial determination that ICANN reasonably deems as the substantive equivalent of any of the foregoing and such member is not removed from Registrar's board of directors or similar governing body within thirty (30) days of Registrar's knowledge of the foregoing.

5.5.4 Registrar fails to cure any breach of this Agreement within twenty-one (21) days after ICANN gives Registrar notice of the breach.

5.5.5 Registrar fails to comply with a ruling granting specific performance under Sections 5.7 or 7.1.

5.5.6 Registrar has been in fundamental and material breach of its obligations under this Agreement at least three (3) times within a twelve (12) month period.

5.5.7 Registrar continues acting in a manner that ICANN has reasonably determined endangers the stability or operational integrity of the Internet after receiving three (3) days notice of that determination.

5.5.8 (i) Registrar makes an assignment for the benefit of creditors or similar act; (ii) attachment, garnishment or similar proceedings are commenced against Registrar, which proceedings are a material threat to Registrar's ability to provide Registrar Services for gTLDs, and are not

dismissed within sixty (60) days of their commencement; (iii) a trustee, receiver, liquidator or equivalent is appointed in place of Registrar or maintains control over any of Registrar's property; (iv) execution is levied upon any property of Registrar, (v) proceedings are instituted by or against Registrar under any bankruptcy, insolvency, reorganization or other laws relating to the relief of debtors and such proceedings are not dismissed within thirty (30) days of their commencement, or (vi) Registrar files for protection under the United States Bankruptcy Code, 11 U.S.C. Section 101 et seq., or a foreign equivalent or liquidates, dissolves or otherwise discontinues its operations.

5.6 Termination Procedures. This Agreement may be terminated in circumstances described in Subsections 5.5.1 though 5.5.6 above only upon fifteen (15) days written notice to Registrar (in the case of Subsection 5.5.4 occurring after Registrar's failure to cure), with Registrar being given an opportunity during that time to initiate arbitration under Subsection 5.8 to determine the appropriateness of termination under this Agreement. This Agreement may be terminated immediately upon notice to Registrar in circumstances described in Subsections 5.5.7 and 5.5.8.

5.7 Suspension.

5.7.1 Upon the occurrence of any of the circumstances set forth in Section 5.5, ICANN may, in ICANN's sole discretion, upon delivery of a notice pursuant to Subsection 5.7.2, elect to suspend Registrar's ability to create or sponsor new Registered Names or initiate inbound transfers of Registered Names for any or all gTLDs for a period of up to a twelve (12) months following the effectiveness of such suspension. Suspension of a Registrar does not preclude ICANN's ability to issue a notice of termination in accordance with the notice requirements of Section 5.6.

5.7.2 Any suspension under Subsections 5.7.1 will be effective upon fifteen (15) days written notice to Registrar, with Registrar being given an opportunity during that time to initiate arbitration under Subsection 5.8 to determine the appropriateness of suspension under this Agreement.

5.7.3 Upon suspension, Registrar shall notify users, by posting a prominent notice on its web site, that it is unable to create or sponsor new gTLD domain name registrations or initiate inbound transfers of Registered Names. Registrar's notice shall include a link to the notice of suspension from ICANN.

5.7.4 If Registrar acts in a manner that ICANN reasonably determines endangers the stability or operational integrity of the Internet and upon notice does not immediately cure, ICANN may suspend this Agreement for five (5) working days pending ICANN's application for more extended specific performance or injunctive relief under Subsection 7.1. Suspension

of the Agreement under this Subsection may, at ICANN's sole discretion, preclude the Registrar from (i) providing Registration Services for gTLDs delegated by ICANN on or after the date of delivery of such notice to Registrar and (ii) creating or sponsoring new Registered Names or initiating inbound transfers of Registered Names for any gTLDs. Registrar must also post the statement specified in Subsection 5.7.3.

5.8 Resolution of Disputes Under this Agreement. Subject to the limitations set forth in Section 6 and Section 7.4, disputes arising under or in connection with this Agreement, including (1) disputes arising from ICANN's failure to renew Registrar's Accreditation and (2) requests for specific performance, shall be resolved in a court of competent jurisdiction or, at the election of either party, by an arbitration conducted as provided in this Subsection 5.8 pursuant to the International Arbitration Rules of the American Arbitration Association ("AAA"). The arbitration shall be conducted in English and shall occur in Los Angeles County, California, USA. Except as set forth in Section 7.4.5, there shall be one (1) arbitrator agreed by the parties from a list of AAA arbitrators, or if parties do not agree on an arbitrator within fifteen (15) days of the AAA request that the parties designate an arbitrator, the AAA shall choose and appoint an arbitrator, paying due regard to the arbitrator's knowledge of the DNS. The parties shall bear the costs of the arbitration in equal shares, subject to the right of the arbitrator to reallocate the costs in their award as provided in the AAA rules. The parties shall bear their own attorneys' fees in connection with the arbitration, and the arbitrator may not reallocate the attorneys' fees in conjunction with their award. The arbitrator shall render its decision within ninety (90) days of the conclusion of the arbitration hearing. In the event Registrar initiates arbitration to contest the appropriateness of termination of this Agreement by ICANN pursuant to Section 5.5 or suspension of Registrar by ICANN pursuant to Section 5.7.1, Registrar may at the same time request that the arbitration panel stay the termination or suspension until the arbitration decision is rendered. The arbitration panel shall order a stay: (i) upon showing by Registrar that continued operations would not be harmful to consumers or the public interest, or (ii) upon appointment by the arbitration panel of a qualified third party to manage the operations of the Registrar until the arbitration decision is rendered. In furtherance of sub-clause (ii) above, the arbitration panel is hereby granted all necessary authority to appoint a qualified third-party to manage the operations of the Registrar upon the Registrar's request and if the panel deems it appropriate. In selecting the third-party manager, the arbitration panel shall take into consideration, but shall not be bound by, any expressed preferences of Registrar. Any order granting a request for a stay must be issued within fourteen (14) days after the filing of the arbitration. If an order granting a request for a stay is not issued within fourteen (14) days, ICANN has the right to proceed with the termination of this Agreement pursuant to Section 5.5 or suspension of the Registrar pursuant to Section 5.7.1. In the event Registrar initiates arbitration to contest an Independent Review Panel's decision under Subsection 4.3.3 sustaining the ICANN Board of Director's determination that a specification or policy is supported by consensus, Registrar may at the same time request that the arbitration

panel stay the requirement that it comply with the policy until the arbitration decision is rendered, and that request shall have the effect of staying the requirement until the decision or until the arbitration panel has granted an ICANN request for lifting of the stay. In all litigation involving ICANN concerning this Agreement (whether in a case where arbitration has not been elected or to enforce an arbitration award), jurisdiction and exclusive venue for such litigation shall be in a court located in Los Angeles, California, USA; however, the parties shall also have the right to enforce a judgment of such a court in any court of competent jurisdiction. For the purpose of aiding the arbitration and/or preserving the rights of the parties during the pendency of an arbitration, the parties shall have the right to seek temporary or preliminary injunctive relief from the arbitration panel or in a court located in Los Angeles, California, USA, which shall not be a waiver of this arbitration agreement.

5.9 Limitations on Monetary Remedies for Violations of this Agreement. ICANN's aggregate monetary liability for violations of this Agreement shall not exceed an amount equal to the Accreditation fees paid by Registrar to ICANN under Subsection 3.9 of this Agreement during the preceding twelve-month period. Registrar's monetary liability to ICANN for violations of this Agreement shall be limited to Accreditation fees owing to ICANN under this Agreement and, except in the case of a good faith disagreement concerning the interpretation of this agreement, reasonable payment to ICANN for the reasonable and direct costs including attorney fees, staff time, and other related expenses associated with legitimate efforts to enforce Registrar compliance with this agreement and costs incurred by ICANN to respond to or mitigate the negative consequences of such behavior for Registered Name Holders and the Internet community. In the event of repeated willful material breaches of the agreement, Registrar shall be liable for sanctions of up to five (5) times ICANN's enforcement costs, but otherwise in no event shall either party be liable for special, indirect, incidental, punitive, exemplary, or consequential damages for any violation of this Agreement.

6. AMENDMENT AND WAIVER.

6.1 If the ICANN Board of Directors determines that an amendment to this Agreement (including to the Specifications referred to herein, unless such Specifications expressly do not permit amendment thereto) and all other registrar agreements between ICANN and the Applicable Registrars (the "Applicable Registrar Agreements") is desirable (each, a "Special Amendment"), ICANN may adopt a Special Amendment pursuant to the requirements of and process set forth in this Section 6; provided that a Special Amendment may not be a Restricted Amendment.

6.2 Prior to submitting a Special Amendment for Registrar Approval, ICANN shall first consult in good faith with the Working Group regarding the form and substance of such Special Amendment. The duration of such consultation shall be reasonably determined by ICANN based on the substance of the Special Amendment. Following

such consultation, ICANN may propose the adoption of a Special Amendment by publicly posting such amendment on its website for no less than thirty (30) calendar days (the "Posting Period") and providing notice of such proposed amendment to the Applicable Registrars in accordance with Section 7.6. ICANN will consider the public comments submitted on a Special Amendment during the Posting Period (including comments submitted by the Applicable Registrars).

6.3 If, within one hundred eighty (180) calendar days following the expiration of the Posting Period (the "Approval Period"), the ICANN Board of Directors approves a Special Amendment (which may be in a form different than submitted for public comment, but must address the subject matter of the Special Amendment posted for public comment, as modified to reflect and/or address input from the Working Group and public comments), ICANN shall provide notice of, and submit, such Special Amendment for approval or disapproval by the Applicable Registrars. If, during the sixty (60) calendar day period following the date ICANN provides such notice to the Applicable Registrars, such Special Amendment receives Registrar Approval, such Special Amendment shall be deemed approved (an "Approved Amendment") by the Applicable Registrars, and shall be effective and deemed an amendment to this Agreement on the date that is sixty (60) calendar days following the date ICANN provided notice of the approval of such Approved Amendment to Registrar (the "Amendment Effective Date"). In the event that a Special Amendment does not receive Registrar Approval, the Special Amendment shall be deemed not approved by the Applicable Registrars (a "Rejected Amendment"). A Rejected Amendment will have no effect on the terms and conditions of this Agreement, except as set forth below.

6.4 If the ICANN Board of Directors reasonably determines that a Rejected Amendment falls within the subject matter categories set forth in Section 1.2 of the Consensus Policies and Temporary Policies Specification, the ICANN Board of Directors may adopt a resolution (the date such resolution is adopted is referred to herein as the "Resolution Adoption Date") requesting an Issue Report (as such term is defined in ICANN's Bylaws) by the Generic Names Supporting Organization (the "GNSO") regarding the substance of such Rejected Amendment. The policy development process undertaken by the GNSO pursuant to such requested Issue Report is referred to herein as a "PDP." If such PDP results in a Final Report supported by a GNSO Supermajority (as defined in ICANN's Bylaws) that either (i) recommends adoption of the Rejected Amendment as Consensus Policy or (ii) recommends against adoption of the Rejected Amendment as Consensus Policy, and, in the case of (i) above, the Board adopts such Consensus Policy, Registrar shall comply with its obligations pursuant to Section 4 of this Agreement. In either case, ICANN will abandon the Rejected Amendment and it will have no effect on the terms and conditions of this Agreement. Notwithstanding the foregoing provisions of this Section 6.4, the ICANN Board of Directors shall not be required to initiate a PDP with respect to a Rejected Amendment if, at any time in the twelve (12) month period preceding the submission of such Rejected Amendment for Registrar Approval pursuant to Section 6.3, the subject matter of such Rejected Amendment was the

subject of a concluded or otherwise abandoned or terminated PDP that did not result in a GNSO Supermajority recommendation.

6.5 If (i) a Rejected Amendment does not fall within the subject matter categories set forth in Section 1.2 of the Consensus Policies and Temporary Policies Specification , (ii) the subject matter of a Rejected Amendment was, at any time in the twelve (12) month period preceding the submission of such Rejected Amendment for Registrar Approval pursuant to Section 6.3, the subject of a concluded or otherwise abandoned or terminated PDP that did not result in a GNSO Supermajority recommendation, or (iii) a PDP does not result in a Final Report supported by a GNSO Supermajority that either (a) recommends adoption of the Rejected Amendment as Consensus Policy or (b) recommends against adoption of the Rejected Amendment as Consensus Policy (or such PDP has otherwise been abandoned or terminated for any reason), then, in any such case, such Rejected Amendment may still be adopted and become effective in the manner described below. In order for the Rejected Amendment to be adopted, the following requirements must be satisfied:

6.5.1 the subject matter of the Rejected Amendment must be within the scope of ICANN's mission and consistent with a balanced application of its core values (as described in ICANN's Bylaws);

6.5.2 the Rejected Amendment must be justified by a Substantial and Compelling Reason in the Public Interest, must be likely to promote such interest, taking into account competing public and private interests that are likely to be affected by the Rejected Amendment, and must be narrowly tailored and no broader than reasonably necessary to address such Substantial and Compelling Reason in the Public Interest;

6.5.3 to the extent the Rejected Amendment prohibits or requires conduct or activities, imposes material costs on the Applicable Registrars, and/or materially reduces public access to domain name services, the Rejected Amendment must be the least restrictive means reasonably available to address the Substantial and Compelling Reason in the Public Interest;

6.5.4 the ICANN Board of Directors must submit the Rejected Amendment, along with a written explanation of the reasoning related to its determination that the Rejected Amendment meets the requirements set out in subclauses (i) through (iii) above, for public comment for a period of no less than thirty (30) calendar days; and

6.5.5 following such public comment period, the ICANN Board of Directors must (i) engage in consultation (or direct ICANN management to engage in consultation) with the Working Group, subject matter experts, members of the GNSO, relevant advisory committees and other interested stakeholders with respect to such Rejected Amendment for a period of no less than sixty

(60) calendar days; and (ii) following such consultation, reapprove the Rejected Amendment (which may be in a form different than submitted for Registrar Approval, but must address the subject matter of the Rejected Amendment, as modified to reflect and/or address input from the Working Group and public comments) by the affirmative vote of at least two-thirds of the members of the ICANN Board of Directors eligible to vote on such matter, taking into account any ICANN policy affecting such eligibility, including ICANN's Conflict of Interest Policy (a "Board Amendment").

Such Board Amendment shall, subject to Section 6.6, be deemed an Approved Amendment, and shall be effective and deemed an amendment to this Agreement on the date that is sixty (60) calendar days following the date ICANN provided notice of the approval of such Board Amendment to Registrar (which effective date shall be deemed the Amendment Effective Date hereunder). Notwithstanding the foregoing, a Board Amendment may not amend the registrar fees charged by ICANN hereunder, or amend this Section 6.

6.6 Notwithstanding the provisions of Section 6.5, a Board Amendment shall not be deemed an Approved Amendment if, during the thirty (30) calendar day period following the approval by the ICANN Board of Directors of the Board Amendment, the Working Group, on the behalf of the Applicable Registrars, submits to the ICANN Board of Directors an alternative to the Board Amendment (an "Alternative Amendment") that meets the following requirements:

6.6.1 sets forth the precise text proposed by the Working Group to amend this Agreement in lieu of the Board Amendment;

6.6.2 addresses the Substantial and Compelling Reason in the Public Interest identified by the ICANN Board of Directors as the justification for the Board Amendment; and

6.6.3 compared to the Board Amendment is: (a) more narrowly tailored to address such Substantial and Compelling Reason in the Public Interest, and (b) to the extent the Alternative Amendment prohibits or requires conduct or activities, imposes material costs on Affected Registrars, or materially reduces access to domain name services, is a less restrictive means to address the Substantial and Compelling Reason in the Public Interest.

Any proposed amendment that does not meet the requirements of subclauses 6.6.1 through 6.6.3 in the immediately preceding sentence shall not be considered an Alternative Amendment hereunder and therefore shall not supersede or delay the effectiveness of the Board Amendment. If, following the submission of the Alternative Amendment to the ICANN Board of Directors, the Alternative Amendment receives Registrar Approval, the Alternative Amendment shall supersede the Board Amendment and shall be deemed an Approved Amendment hereunder (and shall be effective and deemed an amendment to this Agreement on

the date that is sixty (60) calendar days following the date ICANN provided notice of the approval of such Alternative Amendment to Registrar, which effective date shall deemed the Amendment Effective Date hereunder), unless, within a period of sixty (60) calendar days following the date that the Working Group notifies the ICANN Board of Directors of Registrar Approval of such Alternative Amendment (during which time ICANN shall engage with the Working Group with respect to the Alternative Amendment), the ICANN Board of Directors by the affirmative vote of at least two-thirds of the members of the ICANN Board of Directors eligible to vote on such matter, taking into account any ICANN policy affecting such eligibility, including ICANN's Conflict of Interest Policy, rejects the Alternative Amendment. If (A) the Alternative Amendment does not receive Registrar Approval within thirty (30) days of submission of such Alternative Amendment to the Applicable Registrars (and the Working Group shall notify ICANN of the date of such submission), or (B) the ICANN Board of Directors rejects the Alternative Amendment by such two-thirds vote, the Board Amendment (and not the Alternative Amendment) shall be effective and deemed an amendment to this Agreement on the date that is sixty (60) calendar days following the date ICANN provided notice to Registrar (which effective date shall deemed the Amendment Effective Date hereunder). If the ICANN Board of Directors rejects an Alternative Amendment, the board shall publish a written rationale setting forth its analysis of the criteria set forth in Sections 6.6.1 through 6.6.3. The ability of the ICANN Board of Directors to reject an Alternative Amendment hereunder does not relieve the Board of the obligation to ensure that any Board Amendment meets the criteria set forth in Section 6.5.1 through 6.5.5.

6.7 In the event that Registrar believes an Approved Amendment does not meet the substantive requirements set out in this Section 6 or has been adopted in contravention of any of the procedural provisions of this Section 6, Registrar may challenge the adoption of such Special Amendment pursuant to the dispute resolution provisions set forth in Section 5.8, except that such arbitration shall be conducted by a three-person arbitration panel. Any such challenge must be brought within sixty (60) calendar days following the date ICANN provided notice to Registrar of the Approved Amendment, and ICANN may consolidate all challenges brought by registrars (including Registrar) into a single proceeding. The Approved Amendment will be deemed not to have amended this Agreement during the pendency of the dispute resolution process.

6.8 Registrar may apply in writing to ICANN for an exemption from the Approved Amendment (each such request submitted by Registrar hereunder, an "Exemption Request") during the thirty (30) calendar day period following the date ICANN provided notice to Registrar of such Approved Amendment.

6.8.1 Each Exemption Request will set forth the basis for such request and provide detailed support for an exemption from the Approved Amendment. An Exemption Request may also include a detailed description and support for any alternatives to, or a variation of, the Approved Amendment proposed by such Registrar.

6.8.2 An Exemption Request may only be granted upon a clear and convincing showing by Registrar that compliance with the Approved Amendment conflicts with applicable laws or would have a material adverse effect on the long-term financial condition or results of operations of Registrar. No Exemption Request will be granted if ICANN determines, in its reasonable discretion, that granting such Exemption Request would be materially harmful to registrants or result in the denial of a direct benefit to registrants.

6.8.3 Within ninety (90) calendar days of ICANN's receipt of an Exemption Request, ICANN shall either approve (which approval may be conditioned or consist of alternatives to or a variation of the Approved Amendment) or deny the Exemption Request in writing, during which time the Approved Amendment will not amend this Agreement.

6.8.4 If the Exemption Request is approved by ICANN, the Approved Amendment will not amend this Agreement; provided, that any conditions, alternatives or variations of the Approved Amendment required by ICANN shall be effective and, to the extent applicable, will amend this Agreement as of the Amendment Effective Date. If such Exemption Request is denied by ICANN, the Approved Amendment will amend this Agreement as of the Amendment Effective Date (or, if such date has passed, such Approved Amendment shall be deemed effective immediately on the date of such denial), provided that Registrar may, within thirty (30) calendar days following receipt of ICANN's determination, appeal ICANN's decision to deny the Exemption Request pursuant to the dispute resolution procedures set forth in Section 5.8.

6.8.5 The Approved Amendment will be deemed not to have amended this Agreement during the pendency of the dispute resolution process. For avoidance of doubt, only Exemption Requests submitted by Registrar that are approved by ICANN pursuant to this Article 6 or through an arbitration decision pursuant to Section 5.8 shall exempt Registrar from any Approved Amendment, and no Exemption Request granted to any other Applicable Registrar (whether by ICANN or through arbitration), shall have any effect under this Agreement or exempt Registrar from any Approved Amendment.

6.9 Except as set forth in Section 4, Subsection 5.3, this Section 6, Section 7.4 and as otherwise set forth in this Agreement and the Specifications hereto, no amendment, supplement or modification of this Agreement or any provision hereof shall be binding unless executed in writing by both parties, and nothing in this Section 6 or Section 7.4 shall restrict ICANN and Registrar from entering into bilateral amendments and modifications to this Agreement negotiated solely between the two parties. No waiver of any provision of this Agreement shall be binding unless evidenced by a writing signed by the party waiving compliance with such provision. No waiver of any of the provisions of this Agreement or failure to

enforce any of the provisions hereof shall be deemed or shall constitute a waiver of any other provision hereof, nor shall any such waiver constitute a continuing waiver unless otherwise expressly provided. For the avoidance of doubt, nothing in this Section 6 or Section 7.4 shall be deemed to limit Registrar's obligation to comply with Section 4.

6.10 Notwithstanding anything in this Section 6 to the contrary, (a) if Registrar provides evidence to ICANN's reasonable satisfaction that the Approved Amendment would materially increase the cost of providing Registrar Services, then ICANN will allow up to one-hundred eighty (180) calendar days for the Approved Amendment to become effective with respect to Registrar, and (b) no Approved Amendment adopted pursuant to Section 6 shall become effective with respect to Registrar if Registrar provides ICANN with an irrevocable notice of termination pursuant to Section 5.4.

7. MISCELLANEOUS PROVISIONS.

7.1 Specific Performance. While this Agreement is in effect, either party may seek specific performance of any provision of this Agreement in the manner provided in Section 5.8, provided the party seeking such performance is not in material breach of its obligations.

7.2 Handling by ICANN of Registrar-Supplied Data. Before receiving any Personal Data from Registrar, ICANN shall specify to Registrar in writing the purposes for and conditions under which ICANN intends to use the Personal Data. ICANN may from time to time provide Registrar with a revised specification of such purposes and conditions, which specification shall become effective no fewer than thirty (30) days after it is provided to Registrar. ICANN shall not use Personal Data provided by Registrar for a purpose or under conditions inconsistent with the specification in effect when the Personal Data was provided. ICANN shall take reasonable steps to avoid uses of the Personal Data by third parties inconsistent with the specification.

7.3 Assignment; Change of Ownership or Management.

7.3.1 Except as set forth in this Section 7.3.1, either party may assign or transfer this Agreement only with the prior written consent of the other party, which shall not be unreasonably withheld. If ICANN fails to expressly provide or withhold its consent to any requested assignment (an "Assignment Request") of this Agreement by Registrar within thirty (30) calendar days of ICANN's receipt of notice of such Assignment Request (or, if ICANN has requested additional information from Registrar in connection with its review of such request, sixty (60) calendar days of the receipt of all requested written information regarding such request) from Registrar, ICANN shall be deemed to have consented to such requested assignment. Notwithstanding the foregoing, (i) ICANN may assign this Agreement without the consent of Registrar upon approval of the ICANN Board of Directors in conjunction with

a reorganization, reconstitution or re-incorporation of ICANN upon such assignee's express assumption of the terms and conditions of this Agreement, (ii) Registrar may assign this Agreement without the consent of ICANN to a wholly-owned subsidiary of Registrar upon such subsidiary's express assumption of the terms and conditions of this Agreement, and (iii) ICANN shall be deemed to have consented to an Assignment Request in which the assignee associated with such Assignment Request is a party to a Registrar Accreditation Agreement with ICANN on the terms set forth in this Agreement (provided that such assignee is then in compliance with the terms and conditions of such Registrar Accreditation Agreement in all material respects), unless ICANN provides to Registrar a written objection to such Assignment Request within ten (10) calendar days of ICANN's receipt of notice of such Assignment Request pursuant to this Section 7.3.1.

7.3.2 To the extent that an entity acquires a Controlling interest in Registrar's stock, assets or business, Registrar shall provide ICANN notice within seven (7) days of such an acquisition. Such notification shall include a statement that affirms that Registrar meets the Specification or Policy on Accreditation criteria then in effect, and is in compliance with its obligations under this Agreement. Within thirty (30) days of such notification, ICANN may request additional information from the Registrar establishing compliance with this Agreement, in which case Registrar must supply the requested information within fifteen (15) days. Any disputes concerning Registrar's continued Accreditation shall be resolved pursuant to Section 5.8.

7.4 Negotiation Process.

7.4.1 If either the Chief Executive Officer of ICANN ("CEO") or the Chairperson of the Registrar Stakeholder Group ("Chair") desires to discuss any revision(s) to this Agreement, the CEO or Chair, as applicable, shall provide written notice to the other person, which shall set forth in reasonable detail the proposed revisions to this Agreement (a "Negotiation Notice"). Notwithstanding the foregoing, neither the CEO nor the Chair may (i) propose revisions to this Agreement that modify any Consensus Policy then existing, (ii) propose revisions to this Agreement pursuant to this Section 7.4 on or before June 30, 2014, or (iii) propose revisions or submit a Negotiation Notice more than once during any twelve month period beginning on July 1, 2014.

7.4.2 Following receipt of the Negotiation Notice by either the CEO or the Chair, ICANN and the Working Group shall consult in good faith negotiations regarding the form and substance of the proposed revisions to this Agreement, which shall be in the form of a proposed amendment to this Agreement (the "Proposed Revisions"), for a period of at least ninety (90) calendar days (unless a resolution is earlier reached) and attempt to reach a mutually acceptable agreement relating to the Proposed Revisions (the "Discussion Period").

7.4.3 If, following the conclusion of the Discussion Period, an agreement is reached on the Proposed Revisions, ICANN shall post the mutually agreed Proposed Revisions on its website for public comment for no less than thirty (30) calendar days (the "Posting Period") and provide notice of such revisions to all Applicable Registrars in accordance with Section 7.6. ICANN and the Working Group will consider the public comments submitted on the Proposed Revisions during the Posting Period (including comments submitted by the Applicable Registrars). Following the conclusion of the Posting Period, the Proposed Revisions shall be submitted for Registrar Approval and approval by the ICANN Board of Directors. If such approvals are obtained, the Proposed Revisions shall be deemed an Approved Amendment by the Applicable Registrars and ICANN, and shall be effective and deemed an amendment to this Agreement upon sixty (60) calendar days notice from ICANN to Registrar.

7.4.4 If, following the conclusion of the Discussion Period, an agreement is not reached between ICANN and the Working Group on the Proposed Revisions, either the CEO or the Chair may provide the other person written notice (the "Mediation Notice") requiring each party to attempt to resolve the disagreements related to the Proposed Revisions through impartial, facilitative (non-evaluative) mediation in accordance with the terms and conditions set forth below. In the event that a Mediation Notice is provided, ICANN and the Working Group shall, within fifteen (15) calendar days thereof, simultaneously post the text of their desired version of the Proposed Revisions and a position paper with respect thereto on ICANN's website.

7.4.4.1 The mediation shall be conducted by a single mediator selected by the parties. If the parties cannot agree on a mediator within fifteen (15) calendar days following receipt by the CEO or Chair, as applicable, of the Mediation Notice, the parties will promptly select a mutually acceptable mediation provider entity, which entity shall, as soon as practicable following such entity's selection, designate a mediator, who is a licensed attorney with general knowledge of contract law and, to the extent necessary to mediate the particular dispute, general knowledge of the domain name system. Any mediator must confirm in writing that he or she is not, and will not become during the term of the mediation, an employee, partner, executive officer, director, or security holder of ICANN or an Applicable Registrar. If such confirmation is not provided by the appointed mediator, then a replacement mediator shall be appointed pursuant to this Section 7.4.4.1.

7.4.4.2 The mediator shall conduct the mediation in accordance with the rules and procedures for facilitative mediation that he or she determines following consultation with the parties. The parties shall

discuss the dispute in good faith and attempt, with the mediator's assistance, to reach an amicable resolution of the dispute.

7.4.4.3 Each party shall bear its own costs in the mediation. The parties shall share equally the fees and expenses of the mediator.

7.4.4.4 If an agreement is reached during the mediation, ICANN shall post the mutually agreed Proposed Revisions on its website for the Posting Period and provide notice to all Applicable Registrars in accordance with Section 7.6. ICANN and the Working Group will consider the public comments submitted on the agreed Proposed Revisions during the Posting Period (including comments submitted by the Applicable Registrars). Following the conclusion of the Posting Period, the Proposed Revisions shall be submitted for Registrar Approval and approval by the ICANN Board of Directors. If such approvals are obtained, the Proposed Revisions shall be deemed an Approved Amendment by the Applicable Registrars and ICANN, and shall be effective and deemed an amendment to this Agreement upon sixty (60) days notice from ICANN to Registrar.

7.4.4.5 If the parties have not resolved the dispute for any reason by the date that is ninety (90) calendar days following receipt by the CEO or Chair, as applicable, of the Mediation Notice, the mediation shall automatically terminate (unless extended by agreement of the parties). The mediator shall deliver to the parties a definition of the issues that could be considered in future arbitration, if invoked. Those issues are subject to the limitations set forth in Section 7.4.5.2 below.

7.4.5 If, following mediation, ICANN and the Working Group have not reached an agreement on the Proposed Revisions, either the CEO or the Chair may provide the other person written notice (an "Arbitration Notice") requiring ICANN and the Applicable Registry Operators to resolve the dispute through binding arbitration in accordance with the arbitration provisions of Section 5.8, subject to the requirements and limitations of this Section 7.4.5.

7.4.5.1 If an Arbitration Notice is sent, the mediator's definition of issues, along with the Proposed Revisions (be those from ICANN, Registrars or both) shall be posted for public comment on ICANN's website for a period of no less than thirty (30) calendar days. ICANN and the Working Group will consider the public comments submitted on the Proposed Revisions during the Posting Period (including comments submitted by the Applicable Registrars), and information regarding such comments and consideration shall be provided to the a three (3) person arbitrator panel. Each party may modify is Proposed Revisions before and after the Posting Period. The arbitration

proceeding may not commence prior to the closing of such public comment period, and ICANN may consolidate all challenges brought by registrars (including Registrar) into a single proceeding. Except as set forth in this Section 7.4.5.1, the arbitration shall be conducted pursuant to Section 5.8.

7.4.5.2 No dispute regarding the Proposed Revisions may be submitted for arbitration to the extent the subject matter of the Proposed Revisions (i) relates to Consensus Policy, (ii) falls within the subject matter categories set forth in Section 1.2 of the Consensus Policies and Temporary Policies Specification , or (iii) seeks to amend any of the following provisions or Specifications of this Agreement: Sections 2, 4 and 6; subsections 3.1, 3.2, 3.3, 3.4, 3.5, 3.7, 3.8, 3.9, 3.14, 3.19, 3.21, 5.1, 5.2 or 5.3; and the Consensus Policies and Temporary Policies Specification, Data Retention Specification, WHOIS Accuracy Program Specification, Registration Data Directory Service (WHOIS) Specification or the Additional Registrar Operation Specification.

7.4.5.3 The mediator will brief the arbitrator panel regarding ICANN and the Working Group's respective proposals relating to the Proposed Revisions.

7.4.5.4 No amendment to this Agreement relating to the Proposed Revisions may be submitted for arbitration by either the Working Group or ICANN, unless, in the case of the Working Group, the proposed amendment has received Registrar Approval and, in the case of ICANN, the proposed amendment has been approved by the ICANN Board of Directors.

7.4.5.5 In order for the arbitrator panel to approve either ICANN or the Working Group's proposed amendment relating to the Proposed Revisions, the arbitrator panel must conclude that such proposed amendment is consistent with a balanced application of ICANN's core values (as described in ICANN's Bylaws) and reasonable in light of the balancing of the costs and benefits to the business interests of the Applicable Registrars and ICANN (as applicable), and the public benefit sought to be achieved by the Proposed Revisions as set forth in such amendment. If the arbitrator panel concludes that either ICANN or the Working Group's proposed amendment relating to the Proposed Revisions meets the foregoing standard, such amendment shall be effective and deemed an amendment to this Agreement upon sixty (60) calendar days notice from ICANN to Registrar and deemed an Approved Amendment hereunder.

7.4.6 With respect to an Approved Amendment relating to an amendment proposed by ICANN, Registrar may apply in writing to ICANN for an exemption from such amendment pursuant to the provisions of Section 6.8.

7.4.7 Notwithstanding anything in this Section 7.4 to the contrary, (a) if Registrar provides evidence to ICANN's reasonable satisfaction that the Approved Amendment would materially increase the cost of providing Registrar Services, then ICANN will allow up to one-hundred eighty (180) calendar days for the Approved Amendment to become effective with respect to Registrar, and (b) no Approved Amendment adopted pursuant to Section 7.4 shall become effective with respect to Registrar if Registrar provides ICANN with an irrevocable notice of termination pursuant to Section 5.4.

7.5 No Third-Party Beneficiaries. This Agreement shall not be construed to create any obligation by either ICANN or Registrar to any non-party to this Agreement, including any Registered Name Holder.

7.6 Notices and Designations. Except as provided in Section 4.4 and Section 6, all notices to be given under this Agreement shall be given in writing at the address of the appropriate party as set forth below, unless that party has given a notice of change of address in writing. Each party shall notify the other party within thirty (30) days of any change to its contact information. Any written notice required by this Agreement shall be deemed to have been properly given when delivered in person, when sent by electronic facsimile with receipt of confirmation of delivery, when scheduled for delivery by internationally recognized courier service, or when delivered by electronic means followed by an affirmative confirmation of receipt by the recipient's facsimile machine or email server. For any notice of a new Specification or Policy established in accordance with this Agreement, Registrar shall be afforded a reasonable period of time after notice of the establishment of such Specification or Policy is e-mailed to Registrar and posted on the ICANN website in which to comply with that specification, policy or program, taking into account any urgency involved. Notices and designations by ICANN under this Agreement shall be effective when written notice of them is deemed given to Registrar.

If to ICANN, addressed to:

Internet Corporation for Assigned Names and Numbers
12025 Waterfront Drive, Suite 300
Los Angeles, California 90094-2536 USA
Attention: Registrar Accreditation Notices
Telephone: 1/310/823-9358
Facsimile: 1/310/823-8649

If to Registrar, addressed to:

[Registrar Name]
[Courier Address]
[Mailing Address]
Attention: [contact person]
Registrar Website URL: [URL]
Telephone: [telephone number]
Facsimile: [fax number]
e-mail: [e-mail address]

7.7 Dates and Times. All dates and times relevant to this Agreement or its performance shall be computed based on the date and time observed in Los Angeles, California, USA.

7.8 Language. All notices, designations, and Specifications or Policies made under this Agreement shall be in the English language.

7.9 Counterparts. This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

7.10 Entire Agreement. Except to the extent (a) expressly provided in a written agreement executed by both parties concurrently herewith or (b) of written assurances provided by Registrar to ICANN in connection with its Accreditation, this Agreement (including the specifications, which form part of it) constitutes the entire agreement of the parties pertaining to the Accreditation of Registrar and supersedes all prior agreements, understandings, negotiations and discussions, whether oral or written, between the parties on that subject.

7.11 Severability. If one or more provisions of this Agreement are held to be unenforceable under applicable law, the parties agree to renegotiate such provision in good faith. In the event that the parties cannot reach a mutually agreeable and enforceable replacement for such provision, then (a) such provision shall be excluded from this Agreement; (b) the balance of this Agreement shall be interpreted as if such provision were so excluded; and (c) the balance of this Agreement shall be enforceable in accordance with its terms.

[signature page follows]

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed in duplicate by their duly authorized representatives.

ICANN	**[Registrar]**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____

Approved by the ICANN Board on 27 June 2013

WHOIS ACCURACY PROGRAM SPECIFICATION

Registrar shall implement and comply with the requirements set forth in this Specification, as well as any commercially practical updates to this Specification that are developed by ICANN and the Registrar Stakeholder Group during the Term of the Registrar Accreditation Agreement.

1. Except as provided for in Section 3 below, within fifteen (15) days of (1) the registration of a Registered Name sponsored by Registrar, (2) the transfer of the sponsorship of a Registered Name to Registrar, or (3) any change in the Registered Name Holder with respect to any Registered Name sponsored by Registrar, Registrar will, with respect to both Whois information and the corresponding customer account holder contact information related to such Registered Name:

    a. Validate the presence of data for all fields required under Subsection 3.3.1 of the Agreement in a proper format for the applicable country or territory.

    b. Validate that all email addresses are in the proper format according to RFC 5322 (or its successors).

    c. Validate that telephone numbers are in the proper format according to the ITU-T E.164 notation for international telephone numbers (or its equivalents or successors).

    d. Validate that postal addresses are in a proper format for the applicable country or territory as defined in UPU Postal addressing format templates, the S42 address templates (as they may be updated) or other standard formats.

    e. Validate that all postal address fields are consistent across fields (for example: street exists in city, city exists in state/province, city matches postal code) where such information is technically and commercially feasible for the applicable country or territory.

    f. Verify:

        i. the email address of the Registered Name Holder (and, if different, the Account Holder) by sending an email requiring an affirmative response through a tool-based authentication method such as providing a unique code that must be returned in a manner designated by the Registrar, or

        ii. the telephone number of the Registered Name Holder (and, if different, the Account Holder) by either (A) calling or sending an SMS to the Registered Name Holder's telephone number providing a unique code that must be returned in a manner designated by the Registrar, or (B) calling the Registered Name Holder's telephone number and requiring the Registered Name Holder to provide a unique code that was sent to the

Registered Name Holder via web, email or postal mail.

In either case, if Registrar does not receive an affirmative response from the Registered Name Holder, Registrar shall either verify the applicable contact information manually or suspend the registration, until such time as Registrar has verified the applicable contact information. If Registrar does not receive an affirmative response from the Account Holder), Registrar shall verify the applicable contact information manually, but is not required to suspend any registration.

2. Except as provided in Section 3 below, within fifteen (15) calendar days after receiving any changes to contact information in Whois or the corresponding customer account contact information related to any Registered Name sponsored by Registrar (whether or not Registrar was previously required to perform the validation and verification requirements set forth in this Specification in respect of such Registered Name), Registrar will validate and, to the extent required by Section 1, verify the changed fields in the manner specified in Section 1 above. If Registrar does not receive an affirmative response from the Registered Name Holder providing the required verification, Registrar shall either verify the applicable contact information manually or suspend the registration, until such time as Registrar has verified the applicable contact information. If Registrar does not receive an affirmative response from the Account Holder, Registrar shall verify the applicable contact information manually, but is not required to suspend any registration.

3. Except as set forth in paragraph 4 below, Registrar is not required to perform the above validation and verification procedures in Section 1(a) through 1(f) above, if Registrar has already successfully completed the validation and verification procedures on the identical contact information and is not in possession of facts or knowledge of circumstances that suggest that the information is no longer valid.

4. If Registrar has any information suggesting that the contact information specified in Section 1(a) through 1(f) above is incorrect (such as Registrar receiving a bounced email notification or non-delivery notification message in connection with compliance with ICANN's Whois Data Reminder Policy or otherwise) for any Registered Name sponsored by Registrar (whether or not Registrar was previously required to perform the validation and verification requirements set forth in this Specification in respect of such Registered Name), Registrar must verify or re-verify, as applicable, the email address(es) as described in Section 1.f (for example by requiring an affirmative response to a Whois Data Reminder Policy notice). If, within fifteen (15) calendar days after receiving any such information, Registrar does not receive an affirmative response from the Registered Name Holder providing the required verification, Registrar shall either verify the applicable contact information manually or suspend the registration, until such time as Registrar has verified the applicable contact information. If, within fifteen (15) calendar days after receiving any such information, Registrar does not receive an affirmative response from the customer paying for the Registered Name, if applicable, providing the required verification, Registrar shall verify the applicable

contact information manually, but is not required to suspend any registration.

5. Upon the occurrence of a Registered Name Holder's willful provision of inaccurate or unreliable WHOIS information, its willful failure promptly to update information provided to Registrar, or its failure to respond for over fifteen (15) calendar days to inquiries by Registrar concerning the accuracy of contact details associated with the Registered Name Holder's registration, Registrar shall either terminate or suspend the Registered Name Holder's Registered Name or place such registration on clientHold and clientTransferProhibited, until such time as Registrar has validated the information provided by the Registered Name Holder.

6. The terms and conditions of this Specification shall be reviewed by ICANN in consultation with the Registrar Stakeholder Group on or about the first anniversary of the date that the form of this Agreement is first executed by a registrar.

7. Nothing within this Specification shall be deemed to require Registrar to perform verification or validation of any customer account holder information where the customer account holder does not have any Registered Names under sponsorship of Registrar.

Approved by the ICANN Board on 27 June 2013

Approved by the ICANN Board on 27 June 2013

WHOIS ACCURACY PROGRAM SPECIFICATION

Registrar shall implement and comply with the requirements set forth in this Specification, as well as any commercially practical updates to this Specification that are developed by ICANN and the Registrar Stakeholder Group during the Term of the Registrar Accreditation Agreement.

1. Except as provided for in Section 3 below, within fifteen (15) days of (1) the registration of a Registered Name sponsored by Registrar, (2) the transfer of the sponsorship of a Registered Name to Registrar, or (3) any change in the Registered Name Holder with respect to any Registered Name sponsored by Registrar, Registrar will, with respect to both Whois information and the corresponding customer account holder contact information related to such Registered Name:

    a. Validate the presence of data for all fields required under Subsection 3.3.1 of the Agreement in a proper format for the applicable country or territory.

    b. Validate that all email addresses are in the proper format according to RFC 5322 (or its successors).

    c. Validate that telephone numbers are in the proper format according to the ITU-T E.164 notation for international telephone numbers (or its equivalents or successors).

    d. Validate that postal addresses are in a proper format for the applicable country or territory as defined in UPU Postal addressing format templates, the S42 address templates (as they may be updated) or other standard formats.

    e. Validate that all postal address fields are consistent across fields (for example: street exists in city, city exists in state/province, city matches postal code) where such information is technically and commercially feasible for the applicable country or territory.

    f. Verify:

        i. the email address of the Registered Name Holder (and, if different, the Account Holder) by sending an email requiring an affirmative response through a tool-based authentication method such as providing a unique code that must be returned in a manner designated by the Registrar, or

        ii. the telephone number of the Registered Name Holder (and, if different, the Account Holder) by either (A) calling or sending an SMS to the Registered Name Holder's telephone number providing a unique code that must be returned in a manner designated by the Registrar, or (B) calling the Registered Name Holder's telephone number and requiring the Registered Name Holder to provide a unique code that was sent to the

Registered Name Holder via web, email or postal mail.

In either case, if Registrar does not receive an affirmative response from the Registered Name Holder, Registrar shall either verify the applicable contact information manually or suspend the registration, until such time as Registrar has verified the applicable contact information. If Registrar does not receive an affirmative response from the Account Holder), Registrar shall verify the applicable contact information manually, but is not required to suspend any registration.

2. Except as provided in Section 3 below, within fifteen (15) calendar days after receiving any changes to contact information in Whois or the corresponding customer account contact information related to any Registered Name sponsored by Registrar (whether or not Registrar was previously required to perform the validation and verification requirements set forth in this Specification in respect of such Registered Name), Registrar will validate and, to the extent required by Section 1, verify the changed fields in the manner specified in Section 1 above. If Registrar does not receive an affirmative response from the Registered Name Holder providing the required verification, Registrar shall either verify the applicable contact information manually or suspend the registration, until such time as Registrar has verified the applicable contact information. If Registrar does not receive an affirmative response from the Account Holder, Registrar shall verify the applicable contact information manually, but is not required to suspend any registration.

3. Except as set forth in paragraph 4 below, Registrar is not required to perform the above validation and verification procedures in Section 1(a) through 1(f) above, if Registrar has already successfully completed the validation and verification procedures on the identical contact information and is not in possession of facts or knowledge of circumstances that suggest that the information is no longer valid.

4. If Registrar has any information suggesting that the contact information specified in Section 1(a) through 1(f) above is incorrect (such as Registrar receiving a bounced email notification or non-delivery notification message in connection with compliance with ICANN's Whois Data Reminder Policy or otherwise) for any Registered Name sponsored by Registrar (whether or not Registrar was previously required to perform the validation and verification requirements set forth in this Specification in respect of such Registered Name), Registrar must verify or re-verify, as applicable, the email address(es) as described in Section 1.f (for example by requiring an affirmative response to a Whois Data Reminder Policy notice). If, within fifteen (15) calendar days after receiving any such information, Registrar does not receive an affirmative response from the Registered Name Holder providing the required verification, Registrar shall either verify the applicable contact information manually or suspend the registration, until such time as Registrar has verified the applicable contact information. If, within fifteen (15) calendar days after receiving any such information, Registrar does not receive an affirmative response from the customer paying for the Registered Name, if applicable, providing the required verification, Registrar shall verify the applicable

contact information manually, but is not required to suspend any registration.

5. Upon the occurrence of a Registered Name Holder's willful provision of inaccurate or unreliable WHOIS information, its willful failure promptly to update information provided to Registrar, or its failure to respond for over fifteen (15) calendar days to inquiries by Registrar concerning the accuracy of contact details associated with the Registered Name Holder's registration, Registrar shall either terminate or suspend the Registered Name Holder's Registered Name or place such registration on clientHold and clientTransferProhibited, until such time as Registrar has validated the information provided by the Registered Name Holder.

6. The terms and conditions of this Specification shall be reviewed by ICANN in consultation with the Registrar Stakeholder Group on or about the first anniversary of the date that the form of this Agreement is first executed by a registrar.

7. Nothing within this Specification shall be deemed to require Registrar to perform verification or validation of any customer account holder information where the customer account holder does not have any Registered Names under sponsorship of Registrar.

REGISTRATION DATA DIRECTORY SERVICE (WHOIS) SPECIFICATION

1. **Registration Data Directory Services.** Until ICANN requires a different protocol, Registrar will operate a WHOIS service available via port 43 in accordance with RFC 3912, and a web-based Directory Service providing free public query-based access to at least the elements set forth in Section 3.3.1.1 through 3.3.1.8 of the Registrar Accreditation Agreement in the format set forth in Section 1.4 of this Specification. ICANN reserves the right to specify alternative formats and protocols, and upon such specification, the Registrar will implement such alternative specification as soon as reasonably practicable.

   Following the publication by the IETF of a Proposed Standard, Draft Standard or Internet Standard and any revisions thereto (as specified in RFC 2026) relating to the web-based directory service as specified in the IETF Web Extensible Internet Registration Data Service working group, Registrar shall implement the directory service specified in any such standard (or any revision thereto) no later than 135 days after such implementation is requested by ICANN. Registrar shall implement internationalized registration data publication guidelines according to the specification published by ICANN following the work of the ICANN Internationalized Registration Data Working Group (IRD-WG) and its subsequent efforts, no later than 135 days after it is approved by the ICANN Board.

   1.1. The format of responses shall follow a semi-free text format outline below, followed by a blank line and a legal disclaimer specifying the rights of Registrar, and of the user querying the database.

   1.2. Each data object shall be represented as a set of key/value pairs, with lines beginning with keys, followed by a colon and a space as delimiters, followed by the value.

   1.3. For fields where more than one value exists, multiple numbered key/value pairs with the same key shall be allowed (for example to list multiple name servers). The first key/value pair after a blank line should be considered the start of a new record, and should be considered as identifying that record, and is used to group data, such as hostnames and IP addresses, or a domain name and registrant information, together.

   1.4. **Domain Name Data:**

      1.4.1. **Query format:** whois –h whois.example-registrar.tld EXAMPLE.TLD

      1.4.2. **Response format:**

The format of responses shall contain all the elements and follow a semi-free text format outline below. Additional data elements can be added at the end of the text

format outlined below. The data element may, at the option of Registrar, be followed by a blank line and a legal disclaimer specifying the rights of Registrar, and of the user querying the database (provided that any such legal disclaimer must be preceded by such blank line).

Domain Name: EXAMPLE.TLD
Registry Domain ID: D1234567-TLD
Registrar WHOIS Server: whois.example-registrar.tld
Registrar URL: http://www.example-registrar.tld
Updated Date: 2009-05-29T20:13:00Z
Creation Date: 2000-10-08T00:45:00Z
Registrar Registration Expiration Date: 2010-10-08T00:44:59Z
Registrar: EXAMPLE REGISTRAR LLC
Registrar IANA ID: 5555555
Registrar Abuse Contact Email: email@registrar.tld
Registrar Abuse Contact Phone: +1.1235551234
Reseller: EXAMPLE RESELLER[1]
Domain Status: clientDeleteProhibited[2]
Domain Status: clientRenewProhibited
Domain Status: clientTransferProhibited
Registry Registrant ID: 5372808-ERL[3]
Registrant Name: EXAMPLE REGISTRANT[4]
Registrant Organization: EXAMPLE ORGANIZATION
Registrant Street: 123 EXAMPLE STREET
Registrant City: ANYTOWN
Registrant State/Province: AP[5]
Registrant Postal Code: A1A1A1[6]
Registrant Country: AA
Registrant Phone: +1.5555551212
Registrant Phone Ext: 1234[7]
Registrant Fax: +1.5555551213
Registrant Fax Ext: 4321
Registrant Email: EMAIL@EXAMPLE.TLD
Registry Admin ID: 5372809-ERL[8]

[1] Data element may be deleted, provided that if the data element is used, it must appear at this location.
[2] Note: all applicable statuses must be displayed in the Whois output.
[3] May be left blank if not available from Registry.
[4] For the Registrant, Admin and Tech contact fields requiring a "Name" or "Organization", the output must include either the name or organization (or both, if available).
[5] All "State/Province" fields may be left blank if not available.
[6] All "Postal Code" fields may be left blank if not available.
[7] All "Phone Ext", "Fax" and "Fax Ext" fields may be left blank if not available.
[8] May be left blank if not available from Registry.

Admin Name: EXAMPLE REGISTRANT ADMINISTRATIVE
Admin Organization: EXAMPLE REGISTRANT ORGANIZATION
Admin Street: 123 EXAMPLE STREET
Admin City: ANYTOWN
Admin State/Province: AP
Admin Postal Code: A1A1A1
Admin Country: AA
Admin Phone: +1.5555551212
Admin Phone Ext: 1234
Admin Fax: +1.5555551213
Admin Fax Ext: 1234
Admin Email: EMAIL@EXAMPLE.TLD
Registry Tech ID: 5372811-ERL[9]
Tech Name: EXAMPLE REGISTRANT TECHNICAL
Tech Organization: EXAMPLE REGISTRANT LLC
Tech Street: 123 EXAMPLE STREET
Tech City: ANYTOWN
Tech State/Province: AP
Tech Postal Code: A1A1A1
Tech Country: AA
Tech Phone: +1.1235551234
Tech Phone Ext: 1234
Tech Fax: +1.5555551213
Tech Fax Ext: 93
Tech Email: EMAIL@EXAMPLE.TLD
Name Server: NS01.EXAMPLE-REGISTRAR.TLD[10]
Name Server: NS02.EXAMPLE-REGISTRAR.TLD
DNSSEC: signedDelegation
URL of the ICANN WHOIS Data Problem Reporting System:
http://wdprs.internic.net/
>>> Last update of WHOIS database: 2009-05-29T20:15:00Z <<<

1.5. The format of the following data fields: domain status, individual and organizational names, address, street, city, state/province, postal code, country, telephone and fax numbers, email addresses, date and times must conform to the mappings specified in EPP RFCs 5730-5734 (or its successors), and IPv6 addresses format should conform to RFC 5952 (or its successor), so that the display of this information (or values returned in WHOIS responses) can be uniformly processed and understood.

2. Service Level Agreement for Registration Data Directory Services (RDDS)

2.1 Definitions

[9] May be left blank if not available from Registry.
[10] All associated nameservers must be listed.

- **IP address.** Refers to IPv4 or IPv6 addresses without making any distinction between the two. When there is need to make a distinction, IPv4 or IPv6 is used.
- **Probes.** Network hosts used to perform tests (see below) that are located at various global locations.
- **RDDS.** Registration Data Directory Services refers to the collective of WHOIS and Web based WHOIS services.
- **RTT.** Round-Trip Time or **RTT** refers to the time measured from the sending of the first bit of the first packet of the sequence of packets needed to make a request until the reception of the last bit of the last packet of the sequence needed to receive the response. If the client does not receive the whole sequence of packets needed to consider the response as received, the request will be considered unanswered.
- **SLR.** Service Level Requirement is the level of service expected for a certain parameter being measured in a Service Level Agreement (SLA).

2.2 Service Level Agreement Matrix

	Parameter	SLR (monthly basis)
RDDS	RDDS availability	less than or equal to 864 min of downtime
	RDDS query RTT	less than or equal to 4000 ms, for at least 95% of the queries
	RDDS update time	less than or equal to 60 min, for at least 95% of the probes

Registrar is encouraged to do maintenance for the different services at the times and dates of statistically lower traffic for each service. Since substantial downtime is already incorporated in the availability metric, planned outages or similar; any downtime, be it for maintenance or due to system failures, will be noted simply as downtime and counted for SLA purposes.

2.2.1 RDDS availability. Refers to the ability of all the RDDS services for the Registrar to respond to queries from an Internet user with appropriate data from the relevant registrar system. If 51% or more of the RDDS testing probes see any of the RDDS services as unavailable during a given time, the RDDS will be considered unavailable.

2.2.2 WHOIS query RTT. Refers to the **RTT** of the sequence of packets from the start of the TCP connection to its end, including the reception of the WHOIS response. If the **RTT** is 5-times or more the corresponding SLR, the **RTT** will be considered undefined.

2.2.3 Web-based-WHOIS query RTT. Refers to the **RTT** of the sequence of packets from the start of the TCP connection to its end, including the

reception of the HTTP response for only one HTTP request. If Registrar implements a multiple-step process to get to the information, only the last step shall be measured. If the **RTT** is 5-times or more the corresponding SLR, the **RTT** will be considered undefined.

2.2.4 RDDS query RTT. Refers to the collective of "**WHOIS query RTT**" and "**Web-based- WHOIS query RTT**".

2.2.5 RDDS update time. Refers to the time measured from the receipt of an EPP confirmation to a transform command on a domain name, host or contact, up until the servers of the RDDS services reflect the changes made.

2.2.6 RDDS test. Means one query sent to a particular "**IP address**" of one of the servers of one of the RDDS services. Queries shall be about existing objects in the registrar system and the responses must contain the corresponding information otherwise the query will be considered unanswered. Queries with an **RTT** 5 times higher than the corresponding SLR will be considered as unanswered. The possible results to an RDDS test are: a number in milliseconds corresponding to the **RTT** or undefined/unanswered.

2.2.7 Measuring RDDS parameters. Every 5 minutes, RDDS probes will select one IP address from all the public-DNS registered "**IP addresses**" of the servers for each RDDS service of the Registrar being monitored and make an "**RDDS test**" to each one. If an "**RDDS test**" result is undefined/unanswered, the corresponding RDDS service will be considered as unavailable from that probe until it is time to make a new test.

2.2.8 Collating the results from RDDS probes. The minimum number of active testing probes to consider a measurement valid is 10 at any given measurement period, otherwise the measurements will be discarded and will be considered inconclusive; during this situation no fault will be flagged against the SLRs.

2.2.9 Placement of RDDS probes. Probes for measuring RDDS parameters shall be placed inside the networks with the most users across the different geographic regions; care shall be taken not to deploy probes behind high propagation-delay links, such as satellite links.

2.3 Covenants of Performance Measurement

Registrar shall not interfere with measurement **Probes**, including any form of preferential treatment of the requests for the monitored services. Registrar shall respond to the measurement tests described in this Specification as it would do with any other request from Internet users (for RDDS).

CONSENSUS POLICIES AND TEMPORARY POLICIES SPECIFICATION

1. **Consensus Policies.**

1.1. "***Consensus Policies***" are those policies established (1) pursuant to the procedure set forth in ICANN's Bylaws and due process, and (2) covering those topics listed in Section 1.2 of this document. The Consensus Policy development process and procedure set forth in ICANN's Bylaws may be revised from time to time in accordance with the process set forth therein.

1.2. Consensus Policies and the procedures by which they are developed shall be designed to produce, to the extent possible, a consensus of Internet stakeholders, including registrars. Consensus Policies shall relate to one or more of the following:

1.2.1. issues for which uniform or coordinated resolution is reasonably necessary to facilitate interoperability, security and/or stability of the Internet, Registrar Services, Registry Services, or the Domain Name System ("DNS");

1.2.2. functional and performance specifications for the provision of Registrar Services;

1.2.3. registrar policies reasonably necessary to implement Consensus Policies relating to a gTLD registry;

1.2.4. resolution of disputes regarding the registration of domain names (as opposed to the use of such domain names, but including where such policies take into account use of the domain names); or

1.2.5. restrictions on cross-ownership of registry operators and registrars or Resellers and regulations and restrictions with respect to registrar and registry operations and the use of registry and registrar data in the event that a registry operator and a registrar or Reseller are affiliated.

1.3. Such categories of issues referred to in Section 1.2 shall include, without limitation:

1.3.1. principles for allocation of registered names in a TLD (e.g., first-come/first-served, timely renewal, holding period after expiration);

1.3.2. prohibitions on warehousing of or speculation in domain names by registries or registrars;

1.3.3. reservation of registered names in a TLD that may not be registered initially or that may not be renewed due to reasons reasonably related to (i) avoidance of confusion among or misleading of users, (ii) intellectual property, or (iii) the technical management of the DNS or the Internet (e.g., establishment of reservations of names from registration);

1.3.4. maintenance of and access to accurate and up-to-date information concerning Registered Names and name servers;

1.3.5. procedures to avoid disruptions of domain name registrations due to suspension or termination of operations by a registry operator or a registrar, including procedures for allocation of responsibility among continuing registrars of the Registered Names sponsored in a TLD by a registrar losing accreditation; and

1.3.6. the transfer of registration data upon a change in registrar sponsoring one or more Registered Names.

1.4. In addition to the other limitations on Consensus Policies, they shall not:

1.4.1. prescribe or limit the price of Registrar Services;

1.4.2. modify the limitations on Temporary Policies (defined below) or Consensus Policies;

1.4.3. modify the provisions in the Registrar Accreditation Agreement regarding terms or conditions for the renewal, termination or amendment of the Registrar Accreditation Agreement or fees paid by Registrar to ICANN; or

1.4.4. modify ICANN's obligations to not apply standards, policies, procedures or practices arbitrarily, unjustifiably, or inequitably and to not single out Registrar for disparate treatment unless justified by substantial and reasonable cause, and exercise its responsibilities in an open and transparent manner.

2. **Temporary Policies.** Registrar shall comply with and implement all specifications or policies established by the ICANN Board of Directors (the "***Board***") on a temporary basis, if adopted by the Board by a vote of at least two-thirds of its members, so long as the Board reasonably determines that such modifications or amendments are justified and that immediate temporary establishment of a specification or policy on the subject is necessary to maintain the stability or security of Registrar Services, Registry Services or the DNS or the Internet ("***Temporary Policies***").

2.1. Such proposed specification or policy shall be as narrowly tailored as feasible to achieve those objectives. In establishing any Temporary Policy, the Board shall state the period of time for which the Temporary Policy is adopted and shall immediately implement the Consensus Policy development process set forth in ICANN's Bylaws.

2.1.1. ICANN shall also issue an advisory statement containing a detailed explanation of its reasons for adopting the Temporary Policy and why the Board believes such Temporary Policy should receive the consensus support of Internet stakeholders.

2.1.2. If the period of time for which the Temporary Policy is adopted exceeds 90 days, the Board shall reaffirm its temporary adoption every 90 days for a total period not to exceed one year, in order to maintain such Temporary Policy in effect until such time as it becomes a Consensus Policy. If the one year period expires or, if during such one year period, the Temporary Policy does not become a Consensus Policy and is not reaffirmed by the Board, Registrar shall no longer be required to comply with or implement such Temporary Policy.

3. **Notice and Conflicts.** Registrar shall be afforded a reasonable period of time following notice of the establishment of a Consensus Policy or Temporary Policy in which to comply with such policy or specification, taking into account any urgency involved. In the event of a conflict between Registrar Services and Consensus Policies or any Temporary Policy, the Consensus Polices or Temporary Policy shall control, but only with respect to subject matter in conflict. For the avoidance of doubt, Consensus Policies that meet the requirements of this Specification may supplement or supersede provisions of the agreements between Registrar and ICANN, but only to the extent that such Consensus Policies relate to the matters set forth in Section 1.2 and 1.3 of this Specification.

SPECIFICATION ON PRIVACY AND PROXY REGISTRATIONS

Until the earlier to occur of (i) January 1, 2017, and (ii) the date ICANN establishes and implements a Privacy and Proxy Accreditation Program as referenced in Section 3.14 of the Registrar Accreditation Agreement, Registrar agrees to comply, and to require its Affiliates and Resellers to comply, with the terms of this Specification, provided that ICANN and the Working Group may mutually agree to extend the term of this Specification. This Specification may not be modified by ICANN or Registrar.

1. Definitions. For the purposes of this Specification, the following definitions shall apply.

   1.1 "P/P Customer" means, regardless of the terminology used by the P/P Provider, the licensee, customer, beneficial user, beneficiary, or other recipient of Privacy Services and Proxy Services.

   1.2 "Privacy Service" is a service by which a Registered Name is registered to its beneficial user as the Registered Name Holder, but for which alternative, reliable contact information is provided by the P/P Provider for display of the Registered Name Holder's contact information in the Registration Data Service (Whois) or equivalent services.

   1.3 "Proxy Service" is a service through which a Registered Name Holder licenses use of a Registered Name to the P/P Customer in order to provide the P/P Customer use of the domain name, and the Registered Name Holder's contact information is displayed in the Registration Data Service (Whois) or equivalent services rather than the P/P Customer's contact information.

   1.4 "P/P Provider" or "Service Provider" is the provider of Privacy/Proxy Services, including Registrar and its Affiliates, as applicable.

2. Obligations of Registrar. For any Proxy Service or Privacy Service offered by the Registrar or its Affiliates, including any of Registrar's or its Affiliates' P/P services distributed through Resellers, and used in connection with Registered Names Sponsored by the Registrar, the Registrar and its Affiliates must require all P/P Providers to follow the requirements described in this Specification and to abide by the terms and procedures published pursuant to this Specification.

   2.1 Disclosure of Service Terms. P/P Provider shall publish the terms and conditions of its service (including pricing), on its website and/or Registrar's website.

2.2 Abuse/Infringement Point of Contact. P/P Provider shall publish a point of contact for third parties wishing to report abuse or infringement of trademarks (or other rights).

2.3 Disclosure of Identity of P/P Provider. P/P Provider shall publish its business contact information on its website and/or Registrar's website.

2.4 Terms of service and description of procedures. The P/P Provider shall publish on its website and/or Registrar's website a copy of the P/P Provider service agreement and description of P/P Provider's procedures for handling the following:

2.4.1 The process or facilities to report abuse of a domain name registration managed by the P/P Provider;

2.4.2 The process or facilities to report infringement of trademarks or other rights of third parties;

2.4.3 The circumstances under which the P/P Provider will relay communications from third parties to the P/P Customer;

2.4.4 The circumstances under which the P/P Provider will terminate service to the P/P Customer;

2.4.5 The circumstances under which the P/P Provider will reveal and/or publish in the Registration Data Service (Whois) or equivalent service the P/P Customer's identity and/or contact data; and

2.4.6 A description of the support services offered by P/P Providers to P/P Customers, and how to access these services.

2.5 Escrow of P/P Customer Information. Registrar shall include P/P Customer contact information in its Registration Data Escrow deposits required by Section 3.6 of the Agreement. P/P Customer Information escrowed pursuant to this Section 2.5 of this Specification may only be accessed by ICANN in the event of the termination of the Agreement or in the event Registrar ceases business operations.

3. Exemptions. Registrar is under no obligation to comply with the requirements of this specification if it can be shown that:

3.1 Registered Name Holder employed the services of a P/P Provider that is not provided by Registrar, or any of its Affiliates;

3.2 Registered Name Holder licensed a Registered Name to another party (i.e., is acting as a Proxy Service) without Registrar's knowledge; or

3.3 Registered Name Holder has used P/P Provider contact data without subscribing to the service or accepting the P/P Provider terms and conditions.

DATA RETENTION SPECIFICATION

1. During the Term of this Agreement, for each Registered Name sponsored by Registrar within a gTLD, Registrar shall collect and securely maintain in its own electronic database (as updated from time to time) the data specified below:

   1.1. Registrar shall collect the following information from registrants at the time of registration of a domain name (a "Registration") and shall maintain that information for the duration of Registrar's sponsorship of the Registration and for a period of two additional years thereafter:

      1.1.1. First and last name or full legal name of registrant;

      1.1.2. First and last name or, in the event registrant is a legal person, the title of the registrant's administrative contact, technical contact, and billing contact;

      1.1.3. Postal address of registrant, administrative contact, technical contact, and billing contact;

      1.1.4. Email address of registrant, administrative contact, technical contact, and billing contact;

      1.1.5. Telephone contact for registrant, administrative contact, technical contact, and billing contact;

      1.1.6. WHOIS information, as set forth in the WHOIS Specification;

      1.1.7. Types of domain name services purchased for use in connection with the Registration; and

      1.1.8. To the extent collected by Registrar, "card on file," current period third party transaction number, or other recurring payment data.

   1.2. Registrar shall collect the following information and maintain that information for no less than one hundred and eighty (180) days following the relevant interaction:

      1.2.1. Information regarding the means and source of payment reasonably necessary for the Registrar to process the Registration transaction, or a transaction number provided by a third party payment processor;

      1.2.2. Log files, billing records and, to the extent collection and maintenance of such records is commercially practicable or consistent with industry-wide generally accepted standard practices within the industries in which Registrar operates, other

records containing communications source and destination information, including, depending on the method of transmission and without limitation: (1) Source IP address, HTTP headers, (2) the telephone, text, or fax number; and (3) email address, Skype handle, or instant messaging identifier, associated with communications between Registrar and the registrant about the Registration; and

1.2.3. Log files and, to the extent collection and maintenance of such records is commercially practicable or consistent with industry-wide generally accepted standard practices within the industries in which Registrar operates, other records associated with the Registration containing dates, times, and time zones of communications and sessions, including initial registration.

2. If, based on the receipt of either (i) a written legal opinion from a nationally recognized law firm in the applicable jurisdiction that states that the collection and/or retention of any data element specified herein by Registrar is reasonably likely to violate applicable law (the "Opinion") or (ii) a ruling of, or written guidance from, a governmental body of competent jurisdiction providing that compliance with the data collection and/or retention requirements of this Specification violates applicable law, Registrar determines in good faith that the collection and/or retention of any data element specified in this Specification violates applicable law, Registrar may provide written notice of such determination to ICANN and request a waiver from compliance with specific terms and conditions of this Specification (a "Waiver Request"). Such written notice shall: (i) specify the relevant applicable law, the allegedly offending data collection and retention elements, the manner in which the collection and/or retention of such data violates applicable law, and a reasonable description of such determination and any other facts and circumstances related thereto, (ii) be accompanied by a copy of the Opinion and governmental ruling or guidance, as applicable, and (iii) be accompanied by any documentation received by Registrar from any governmental authority, in each case, related to such determination, and such other documentation reasonably requested by ICANN. Following receipt of such notice, ICANN and Registrar shall discuss the matter in good faith in an effort to reach a mutually acceptable resolution of the matter. Until such time as ICANN's Procedure for Handling Whois Conflicts with Privacy Law is modified to include conflicts relating to the requirements of this Specification and if ICANN agrees with Registrar's determination, ICANN's office of general counsel may temporarily or permanently suspend compliance and enforcement of the affected provisions of this Specification and grant the Wavier Request. Prior to granting any exemption hereunder, ICANN will post its determination on its website for a period of thirty (30) calendar days. Following such modification of ICANN's Procedure for Handling Whois Conflicts with Privacy Law, all Wavier Requests (whether granted or denied) shall be resolved pursuant to such modified procedures.

3. If (i) ICANN has previously waived compliance with the requirements of any requirement of this Data Retention Specification in response to a Waiver Request from a registrar that is located in the same jurisdiction as Registrar and (ii) Registrar is subject to the same applicable law that gave rise to ICANN's agreement to grant such wavier, Registrar may request that ICANN to grant a similar waiver, which request shall be approved by ICANN, unless ICANN provides Registrar with a reasonable justification for not approving such request, in which case Registrar may thereafter make an Wavier Request pursuant to Section 2 of this Data Retention Specification.

4. Any modification of this Data Retention Specification to address violations of applicable law shall only apply during the period of time that the specific provisions of the applicable law giving rise to such violations remain in effect. If the applicable law is repealed or modified (or preempted) in a manner that would no longer prohibit the collection and/or retention of data and information as originally specified in this Data Retention Specification, Registrar agrees that the original version of this Specification will apply to the maximum extent permitted by such modified applicable law.

REGISTRAR INFORMATION SPECIFICATION

Registrar shall provide to ICANN the information specified below, which shall be maintained in accordance with Section 3.17 of the Agreement. With regard to information identified below, ICANN will hold such information pursuant to the disclosure requirements set forth in Section 3.15 of the Agreement.

General Information

1. Full legal name of Registrar.

2. Legal form of the Registrar (e.g., LLC, Corporation, Government Body, Intergovernmental Organization, etc.).

3. The jurisdiction in which the Registrar's business is registered for legal and financial purposes.

4. The Registrar's business registration number and the name of the authority that issued this number.

5. Every business name and/or trade name used by the Registrar.

6. Provide current documentation demonstrating that the Registrar entity is legally established and in good standing. For proof of establishment, provide charter documents or other equivalent document (e.g., membership agreement) of the entity. If the Registrar is a government body or organization, provide a certified copy of the relevant statute, governmental decision or other instrument under which the government body or organization has been established. With respect to an entity other than a government body or organization, where no such certificates or documents are available in the Registrar's jurisdiction, an affidavit drafted and signed by a notary public or a legal practitioner duly qualified in the courts of the Registrar's jurisdiction, declaring that the organization is established and in good standing, must be provided.

7. Correspondence address for the Registrar.* This address will be used for contractual purposes, and the Registrar must be able to accept notices and service of legal process at this address. No Post Office boxes are allowed.

8. Primary phone number where the Registrar can be reached for contractual purposes.

9. Primary Fax number where the Registrar can be reached for contractual purposes.

10. Primary Email address where the Registrar can be reached for contractual purposes.

11. If the location or address of Registrar's principal place of business is different from the address provided in 7, provide details including address, phone number, fax number and email address.* Provide ICANN with current documentation demonstrating that the Registrar is legally entitled to do business in the principal place of business.

12. Any other addresses where the Registrar will be operated or managed, if different from either its principal place of business or correspondence address provided above. (If so, please explain.) Provide ICANN with current documentation demonstrating that the Registrar is legally entitled to do business in each location identified.

13. Primary contact name:

Title
Address
Phone number
Fax number
Email address

14. URL and Location of Port 43 WHOIS server.

Ownership, Directors and Officers Information

15. Full name, contact information, and position of any persons or entities owning at least 5% of the ownership interest in Registrar's current business entity. For each person listed, please specify such person's percentage ownership.

16. Full name, contact information, and position of all directors of the Registrar.

17. Full name, contact information, and position of all officers of the Registrar.* (Officer names and positions must be publicly displayed.)

18. Full name, contact information, and position of all senior management and other key personnel overseeing the provision of Registrar Services.

19. For every person or entity mentioned in the answers to questions 15 to 18, indicate if that person or entity:

a) within the past ten years, has been convicted of a felony or of a misdemeanor related to financial activities, or has been judged by a court to have committed fraud or breach of fiduciary duty, or has been the subject of a judicial determination that is similar or related to any of these;

b) within the past ten years, has been disciplined by any government or industry regulatory body for conduct involving dishonesty or misuse of funds of others;

c) is currently involved in any judicial or regulatory proceeding that could result in a conviction, judgment, determination, or discipline of the type specified in items 19(a) or 19(b); or

d) is the subject of a disqualification imposed by ICANN.

Provide details if any of the above events in (a)-(d) have occurred.

20. List all Affiliated Registrars, if any, and briefly describe the Affiliation.

21. For any entities listed in item 20, must provide information required in items 1-14 above.

22. List the ultimate parent entity of the Registrar, if applicable.*

Other

23. Does the Registrar or any of its Affiliates offer any Privacy Service or Proxy Service (as such terms on defined in the Specification on Privacy and Proxy Registrations)? If yes, list the entities or individuals providing the Privacy Service or Proxy Service.

24. For any entities listed in item 20, provide information required in 1-14 above.

25. Does the Registrar utilize or benefit from the services of Resellers?

26. If yes, provide a list of all such Resellers known to Registrar. The information specified in this item 26 shall be made available to ICANN upon request. At such time as ICANN develops a secure method for the receipt and retention of such information, such information shall thereafter be provided to ICANN in accordance with Section 3.17 of the Agreement.

ADDITIONAL REGISTRAR OPERATION SPECIFICATION

This Specification may be modified by ICANN from time to time after consultation with the Registrar Stakeholder Group (or its successor), provided that such updates are commercially practical with respect to the registrar industry, taken as a whole.

1. DNSSEC

Registrar must allow its customers to use DNSSEC upon request by relaying orders to add, remove or change public key material (e.g., DNSKEY or DS resource records) on behalf of customers to the Registries that support DNSSEC. Such requests shall be accepted and processed in a secure manner and according to industry best practices. Registrars shall accept any public key algorithm and digest type that is supported by the TLD of interest and appears in the registries posted at: <http://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xml> and <http://www.iana.org/assignments/ds-rr-types/ds-rr-types.xml>. All such requests shall be transmitted to registries using the EPP extensions specified in RFC 5910 or its successors.

2. IPv6

To the extent that Registrar offers registrants the ability to register nameserver addresses, Registrar must allow both IPv4 addresses and IPv6 addresses to be specified.

3. IDN

If the Registrar offers Internationalized Domain Name ("IDN") registrations, all new registrations must comply with RFCs 5890, 5891, 5892, 5893 and their successors. Registrar shall also comply with the IDN Guidelines at http://www.icann.org/en/topics/idn/implementation-guidelines.htm which may be amended, modified, or superseded from time to time. Registrar must use the IDN tables published by the relevant registry.

Registrants' Benefits and Responsibilities

Domain Name Registrants' Rights:

1. Your domain name registration and any privacy/proxy services you may use in conjunction with it must be subject to a Registration Agreement with an ICANN Accredited Registrar.

    - You are entitled to review this Registration Agreement at any time, and download a copy for your records.

2. You are entitled to accurate and accessible information about:

    - The identity of your ICANN Accredited Registrar;
    - The identity of any proxy or privacy service provider affiliated with your Registrar;
    - Your Registrar's terms and conditions, including pricing information, applicable to domain name registrations;
    - The terms and conditions, including pricing information, applicable to any privacy services offered by your Registrar;
    - The customer support services offered by your Registrar and the privacy services provider, and how to access them;
    - How to raise concerns and resolve disputes with your Registrar and any privacy services offered by them; and
    - Instructions that explain your Registrar's processes for registering, managing, transferring, renewing, and restoring your domain name registrations, including through any proxy or privacy services made available by your Registrar.

3. You shall not be subject to false advertising or deceptive practices by your Registrar or though any proxy or privacy services made available by your Registrar. This includes deceptive notices, hidden fees, and any practices that are illegal under the consumer protection law of your residence.

Domain Name Registrants' Responsibilities:

1. You must comply with the terms and conditions posted by your Registrar, including applicable policies from your Registrar, the Registry and ICANN.

2. You must review your Registrar's current Registration Agreement, along with any updates.

3. You will assume sole responsibility for the registration and use of your domain name.

4. You must provide accurate information for publication in directories such as WHOIS, and promptly update this to reflect any changes.

5. You must respond to inquiries from your Registrar within fifteen (15) days, and keep your Registrar account data current. If you choose to have your domain name registration renew automatically, you must also keep your payment information current.

LOGO LICENSE SPECIFICATION to RAA

LOGO LICENSE SPECIFICATION

The Internet Corporation for Assigned Names and Numbers, a California non-profit, public benefit corporation ("ICANN"), and [Registrar Name], a [organization type and jurisdiction] ("Registrar") have entered into a Registrar Accreditation Agreement ("Registrar Accreditation Agreement"), of which this appendix ("Logo License Specification") is a part. Definitions in the Registrar Accreditation Agreement apply in this Logo License Specification.

Registrar wishes to acquire from ICANN, and ICANN wishes to grant to Registrar, a license to use the trademarks listed below the signature block of this Logo License Specification ("Trademarks") in connection with Registrar's role as an ICANN-accredited registrar. Pursuant to and subject to the Registrar Accreditation Agreement, Registrar and ICANN hereby agree as follows:

LICENSE

1. Grant of License. ICANN grants to Registrar a non-exclusive, worldwide right and license to use the Trademarks, during the term of this specification and solely in connection with the provision and marketing of Registrar Services in order to indicate that Registrar is accredited as a registrar of domain names by ICANN. Except as provided in this subsection and Subsection 2.2 of the Registrar Accreditation Agreement, Registrar shall not use the Trademarks, any term, phrase, or design which is confusingly similar to the Trademarks or any portion of the Trademarks in any manner whatsoever.

2. Ownership of Trademarks. Any and all rights in the Trademarks that may be acquired by Registrar shall inure to the benefit of, and are herby assigned to, ICANN. Registrar shall not assert ownership of the Trademarks or any associated goodwill.

3. No Sublicense. Registrar shall not sublicense any of its rights under this specification to any other person or entity (including any of Registrar's resellers) without the prior written approval of ICANN.

REGISTRATION AND ENFORCEMENT

1. Registration. Registration and any other form of protection for the Trademarks shall only be obtained by ICANN in its name and at its expense.

2. Enforcement. Registrar shall promptly notify ICANN of any actual or suspected infringement of the Trademarks by third parties, including Registrar's resellers or affiliates. ICANN shall have the sole discretion to initiate and maintain any legal proceedings against such third parties; Registrar shall not take any such actions without the prior written approval of ICANN; and ICANN shall retain any and all recoveries from such actions.

3. Further Assurances. Registrar agrees to execute such other documents and to take all such actions as ICANN may request to effect the terms of this specification, including providing such materials (for example URLs and samples of any promotional materials bearing the Trademarks), cooperation, and assistance as may be reasonably required to assist ICANN in obtaining, maintaining, and enforcing trademark registration(s) and any other form of protection for the Trademarks.

TERM AND TERMINATION

This Logo License Specification shall be effective from the date it is signed below by both parties until the Expiration Date, unless this specification or the Registrar Accreditation Agreement is earlier terminated. Each party shall have the right to terminate this specification at any time by giving the other party written notice. Upon expiration or termination of this specification, Registrar shall immediately discontinue all use of the Trademarks.

IN WITNESS WHEREOF, the parties have caused this Logo License Specification to be executed by their duly authorized representatives.

ICANN	[Registrar Name]
By: _____	By: _____ Name: Title:
	Dated: _____, 200__

TRADEMARKS:

1. ICANN Accredited Registrar

2.

Approved by the ICANN Board on 27 June 2013

COMPLIANCE CERTIFICATE

_____, 20__

Pursuant to Section 3.15 of Registrar Accreditation Agreement (the "Agreement"), dated _____, 20__, by and between the Internet Corporation for Assigned Names and Numbers, a California non-profit, public benefit corporation ("ICANN"), and [Registrar Name], a [Organization type and jurisdiction] ("Registrar"), the undersigned certifies, in his/her capacity as an officer of the Registrar and not in his/her individual capacity, on behalf of Registrar as follows:

1. The undersigned is the [Chief Executive Officer/President/Chief Operating Officer/Chief Financial Officer or functional equivalent thereof] of Registrar.

2. Registrar has in place processes and procedures intended to establish, maintain, review, test, and modify registrar policies and procedures reasonably designed to achieve compliance with the Agreement.

3. To the best of the undersigned's knowledge and belief, Registrar has performed and complied with all covenants, agreements, obligations and conditions contained in the Agreement that are required to be performed or complied with by it for the calendar year 20__.

The undersigned signs this certificate as of the date indicated under the title.

[REGISTRAR]

By: _____
Name:
Title:

Transition Addendum to Registrar Accreditation Agreement

This Transition Addendum (this "Addendum") to the Registrar Accreditation Agreement (the "Agreement") by and between the Internet Corporation for Assigned Names and Numbers, a California non-profit, public benefit corporation ("ICANN"), and [Registrar Name], a [Organization type and jurisdiction] ("Registrar"), is dated as of _____, 2013.

WHEREAS, ICANN and Registrar entered into the Agreement as of the date hereof; and

WHEREAS, ICANN acknowledges that implementation by Registrar of certain operational provisions of the Agreement is not possible on the date hereof and will require a reasonable grace period.

NOW THEREFORE, the parties agree as follows:

1. ICANN will not enforce the following provisions and specifications of the Agreement until January 1, 2014: Sections 3.4.1.1, 3.4.1.5, 3.7.10, 3.7.11, 3.12.4, 3.12.7, 3.14, 3.18 and 3.19 of the Agreement; the first sentence of Section 3.7.8 of the Agreement; the WHOIS Accuracy Specification; the Data Retention Specification; and the service level agreements set forth in Section 2.2 of the Registration Data Directory Service (WHOIS) Specification (collectively, the "Transition Provisions").

2. In addition, if immediately prior to the execution of this Addendum Registrar was party to the form registrar accreditation agreement adopted by ICANN in 2009 (the "2009 RAA"), Registrar may use its existing form of registrant registration agreement until January 1, 2014, provided that such agreement complies with Section 3.7.7 of the 2009 RAA.

3. For the calendar year ended December 31, 2013, any certification required pursuant to Section 3.15 shall not require certification as to compliance with the Transition Provisions and may acknowledge the permissible use of the registrant registration agreement under Section 2 hereof.

4. Notwithstanding the foregoing, Registrar agrees to use commercially reasonable efforts to comply with the obligations set forth in the Transition Provisions and transition to a registrant registration agreement that complies with the terms of the Agreement prior to January 1, 2014.

5. Registrar must be fully compliant with the Transition Provisions and Section 3.7.7 of the Agreement as of January 1, 2014, at which date this Addendum shall automatically terminate without action by any party, except as it relates to Section 4 hereof.

6. ICANN and the Registrar Whois Validation Working Group (as defined below) will work together to identify and specify an appropriate set of tools to enable Registrar to complete the across field validation specified in Section 1(e) of the Whois Accuracy Program Specification to the Agreement (the "Across Field Validation"). When such tools are mutually agreed between ICANN and the Registrar Whois Validation Working Group,

ICANN shall provide Registrar written notice of such agreement (which notice shall specify and describe the agreed upon tools). Effective on the one hundred eightieth (180th) calendar day following delivery of such notice by ICANN, Registrar shall comply with the obligations specified in Section 1(e) of the Whois Accuracy Program. Until such time, ICANN will not enforce compliance with such obligations.

For purposes of this Section 6, the Registrar Whois Validation Working Group shall be deemed to have agreed to such Across Field Validation tools when Approval (as defined below) of the then serving members of the group is obtained through a vote of the group (which vote may be conducted through any verifiable means determined by the group, including through electronic means).

The "Registrar Whois Validation Working Group" means that existing working group whose membership has been tasked with identifying and specifying a set of tools to enable registrars to complete the Across Field Validation. The membership of the Registrar Whois Validation Working Group shall be made up of volunteering representatives of ICANN-accredited registrars, and shall initially consist of the members currently serving on the existing working group.

"Approval" is obtained following a vote of the Registrar Whois Validation Working Group, if the votes cast in favor of adoption of the proposed Across Field Validations tools by the then serving members of the group are at least two-thirds of the votes cast by such members, with abstentions or non-votes not being counted as either votes in favor or against adoption of such tools. For purposes of the vote of the group as referenced above, (i) only persons appointed by an ICANN-accredited registrar shall be deemed members of the group and eligible to cast a vote as described above and (ii) no ICANN-accredited registrar nor group of Affiliated Registrars represented in the Registrar Whois Validation Working Group shall have more than one vote.

7. Except as set forth in this Addendum, the Agreement shall be in full force and effect, enforceable by the parties in accordance with its terms.

[signature page follows]

IN WITNESS WHEREOF, the parties hereto have caused this Addendum to be executed in duplicate by their duly authorized representatives.

ICANN	**[Registrar]**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____

EXHIBIT 5

Welcome to the new ICANN.org! Learn more, and send us your feedback. ✖ Dismiss

Translations Français Español العربية

Русский 中文 Log In Sign Up

Search ICANN.org

ICANN

GET STARTED NEWS & MEDIA POLICY PUBLIC COMMENT RESOURCES

COMMUNITY IANA STEWARDSHIP & ACCOUNTABILITY

Resources

- About ICANN
- Board
- Accountability & Transparency
- Governance
- Groups
- Contractual Compliance
- Registrars
- Registries

Operational Metrics

- Identifier Systems

Uniform Domain Name Dispute Resolution Policy

This page is available in: العربية | Deutsch | English | Español | Français | Italiano | 日本語 | 한국어 | Português | Русский | 中文

Policy Adopted: August 26, 1999
Implementation Documents Approved: October 24, 1999

Notes:

1. This policy is now in effect. See www.icann.org/udrp/udrp-schedule.htm for the implementation schedule.

2. This policy has been adopted by all ICANN-accredited registrars. It has also been adopted by certain managers of country-code top-level domains (e.g., .nu, .tv, .ws).

3. The policy is between the registrar (or other registration authority in the case of a country-code

Security, Stability and Resiliency (IS-SSR)
- ccTLDs
- Internationalized Domain Names
- Universal Acceptance Initiative
- Policy
- Public Comment
- Contact
- Help
  - Dispute Resolution
  - Domain Name Dispute Resolution
    - Charter Eligibility Dispute Resolution Policy
    - Eligibility Requirements Dispute Resolution Policy
    - Intellectual Property Defensive Registration Challenge Policy

top-level domain) and its customer (the domain-name holder or registrant). Thus, the policy uses "we" and "our" to refer to the registrar and it uses "you" and "your" to refer to the domain-name holder.

Uniform Domain Name Dispute Resolution Policy

(As Approved by ICANN on October 24, 1999)

1. Purpose. This Uniform Domain Name Dispute Resolution Policy (the "Policy") has been adopted by the Internet Corporation for Assigned Names and Numbers ("ICANN"), is incorporated by reference into your Registration Agreement, and sets forth the terms and conditions in connection with a dispute between you and any party other than us (the registrar) over the registration and use of an Internet domain name registered by you. Proceedings under Paragraph 4 of this Policy will be conducted according to the Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules of Procedure"), which are available at http://www.icann.org/en/dndr/udrp/uniform-rules.htm, and the selected administrative-dispute-resolution service provider's supplemental rules.

2. Your Representations. By applying to register a domain name, or by asking us to maintain or renew a domain name registration, you hereby represent and warrant to us that (a) the statements that you made in your Registration Agreement are complete and accurate; (b) to your knowledge, the registration of the domain name will not infringe upon or otherwise violate the rights of any third party; (c) you are not registering the domain name for an unlawful purpose; and (d) you will not knowingly use the domain name in violation of any applicable laws or regulations. It is your responsibility to determine whether your domain name registration infringes or violates someone else's rights.

3. Cancellations, Transfers, and Changes. We will cancel, transfer or otherwise make changes to domain name registrations under the following circumstances:

a. subject to the provisions of Paragraph 8, our receipt of written or appropriate electronic instructions from you or

- Qualification Challenge Policy
- Restrictions Dispute Resolution Policy
- Transfer Dispute Resolution Policy
- Uniform Domain Name Dispute Resolution Policy
  - Policy Document
  - Providers
  - Provider Approval Process
  - Rules
  - Principal Documents
  - Proceedings
  - Historical Documents
  - Timeline
- Name Collision
- Registrar Problems
- Whois Data Correction
- Independent Review Process
- Request for

your authorized agent to take such action;

b. our receipt of an order from a court or arbitral tribunal, in each case of competent jurisdiction, requiring such action; and/or

c. our receipt of a decision of an Administrative Panel requiring such action in any administrative proceeding to which you were a party and which was conducted under this Policy or a later version of this Policy adopted by ICANN. (See Paragraph 4(i) and (k) below.)

We may also cancel, transfer or otherwise make changes to a domain name registration in accordance with the terms of your Registration Agreement or other legal requirements.

4. Mandatory Administrative Proceeding.

This Paragraph sets forth the type of disputes for which you are required to submit to a mandatory administrative proceeding. These proceedings will be conducted before one of the administrative-dispute-resolution service providers listed at www.icann.org/en/dndr/udrp/approved-providers.htm (each, a "Provider").

a. Applicable Disputes. You are required to submit to a mandatory administrative proceeding in the event that a third party (a "complainant") asserts to the applicable Provider, in compliance with the Rules of Procedure, that

(i) your domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and

(ii) you have no rights or legitimate interests in respect of the domain name; and

(iii) your domain name has been registered and is being used in bad faith.

In the administrative proceeding, the complainant must prove that each of these three elements are present.

Reconsideration

b. Evidence of Registration and Use in Bad Faith. For the purposes of Paragraph 4(a)(iii), the following circumstances, in particular but without limitation, if found by the Panel to be present, shall be evidence of the registration and use of a domain name in bad faith:

(i) circumstances indicating that you have registered or you have acquired the domain name primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant who is the owner of the trademark or service mark or to a competitor of that complainant, for valuable consideration in excess of your documented out-of-pocket costs directly related to the domain name; or

(ii) you have registered the domain name in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that you have engaged in a pattern of such conduct; or

(iii) you have registered the domain name primarily for the purpose of disrupting the business of a competitor; or

(iv) by using the domain name, you have intentionally attempted to attract, for commercial gain, Internet users to your web site or other on-line location, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation, or endorsement of your web site or location or of a product or service on your web site or location.

c. How to Demonstrate Your Rights to and Legitimate Interests in the Domain Name in Responding to a Complaint. When you receive a complaint, you should refer to Paragraph 5 of the Rules of Procedure in

determining how your response should be prepared. Any of the following circumstances, in particular but without limitation, if found by the Panel to be proved based on its evaluation of all evidence presented, shall demonstrate your rights or legitimate interests to the domain name for purposes of Paragraph 4(a)(ii):

> (i) before any notice to you of the dispute, your use of, or demonstrable preparations to use, the domain name or a name corresponding to the domain name in connection with a bona fide offering of goods or services; or
>
> (ii) you (as an individual, business, or other organization) have been commonly known by the domain name, even if you have acquired no trademark or service mark rights; or
>
> (iii) you are making a legitimate noncommercial or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trademark or service mark at issue.

d. Selection of Provider. The complainant shall select the Provider from among those approved by ICANN by submitting the complaint to that Provider. The selected Provider will administer the proceeding, except in cases of consolidation as described in Paragraph 4(f).

e. Initiation of Proceeding and Process and Appointment of Administrative Panel. The Rules of Procedure state the process for initiating and conducting a proceeding and for appointing the panel that will decide the dispute (the "Administrative Panel").

f. Consolidation. In the event of multiple disputes between you and a complainant, either you or the complainant may petition to consolidate the disputes before a single Administrative Panel. This petition shall be made to the first Administrative Panel appointed to

hear a pending dispute between the parties. This Administrative Panel may consolidate before it any or all such disputes in its sole discretion, provided that the disputes being consolidated are governed by this Policy or a later version of this Policy adopted by ICANN.

g. Fees. All fees charged by a Provider in connection with any dispute before an Administrative Panel pursuant to this Policy shall be paid by the complainant, except in cases where you elect to expand the Administrative Panel from one to three panelists as provided in Paragraph 5(b)(iv) of the Rules of Procedure, in which case all fees will be split evenly by you and the complainant.

h. Our Involvement in Administrative Proceedings. We do not, and will not, participate in the administration or conduct of any proceeding before an Administrative Panel. In addition, we will not be liable as a result of any decisions rendered by the Administrative Panel.

i. Remedies. The remedies available to a complainant pursuant to any proceeding before an Administrative Panel shall be limited to requiring the cancellation of your domain name or the transfer of your domain name registration to the complainant.

j. Notification and Publication. The Provider shall notify us of any decision made by an Administrative Panel with respect to a domain name you have registered with us. All decisions under this Policy will be published in full over the Internet, except when an Administrative Panel determines in an exceptional case to redact portions of its decision.

k. Availability of Court Proceedings. The mandatory administrative proceeding requirements set forth in Paragraph 4 shall not prevent either you or the complainant from submitting the dispute to a court of competent jurisdiction for independent resolution before such mandatory administrative proceeding is commenced or after such proceeding is concluded. If an

Administrative Panel decides that your domain name registration should be canceled or transferred, we will wait ten (10) business days (as observed in the location of our principal office) after we are informed by the applicable Provider of the Administrative Panel's decision before implementing that decision. We will then implement the decision unless we have received from you during that ten (10) business day period official documentation (such as a copy of a complaint, file-stamped by the clerk of the court) that you have commenced a lawsuit against the complainant in a jurisdiction to which the complainant has submitted under Paragraph 3(b)(xiii) of the Rules of Procedure. (In general, that jurisdiction is either the location of our principal office or of your address as shown in our Whois database. See Paragraphs 1 and 3(b)(xiii) of the Rules of Procedure for details.) If we receive such documentation within the ten (10) business day period, we will not implement the Administrative Panel's decision, and we will take no further action, until we receive (i) evidence satisfactory to us of a resolution between the parties; (ii) evidence satisfactory to us that your lawsuit has been dismissed or withdrawn; or (iii) a copy of an order from such court dismissing your lawsuit or ordering that you do not have the right to continue to use your domain name.

5. All Other Disputes and Litigation. All other disputes between you and any party other than us regarding your domain name registration that are not brought pursuant to the mandatory administrative proceeding provisions of Paragraph 4 shall be resolved between you and such other party through any court, arbitration or other proceeding that may be available.

6. Our Involvement in Disputes. We will not participate in any way in any dispute between you and any party other than us regarding the registration and use of your domain name. You shall not name us as a party or otherwise include us in any such proceeding. In the event that we are named as a party in any such proceeding, we reserve the right to raise any and all defenses deemed appropriate, and to take any other action necessary to defend ourselves.

7. Maintaining the Status Quo. We will not cancel, transfer, activate, deactivate, or otherwise change the status of any domain name registration under this Policy except as provided in Paragraph 3 above.

8. Transfers During a Dispute.

a. Transfers of a Domain Name to a New Holder. You may not transfer your domain name registration to another holder (i) during a pending administrative proceeding brought pursuant to Paragraph 4 or for a period of fifteen (15) business days (as observed in the location of our principal place of business) after such proceeding is concluded; or (ii) during a pending court proceeding or arbitration commenced regarding your domain name unless the party to whom the domain name registration is being transferred agrees, in writing, to be bound by the decision of the court or arbitrator. We reserve the right to cancel any transfer of a domain name registration to another holder that is made in violation of this subparagraph.

b. Changing Registrars. You may not transfer your domain name registration to another registrar during a pending administrative proceeding brought pursuant to Paragraph 4 or for a period of fifteen (15) business days (as observed in the location of our principal place of business) after such proceeding is concluded. You may transfer administration of your domain name registration to another registrar during a pending court action or arbitration, provided that the domain name you have registered with us shall continue to be subject to the proceedings commenced against you in accordance with the terms of this Policy. In the event that you transfer a domain name registration to us during the pendency of a court action or arbitration, such dispute shall remain subject to the domain name dispute policy of the registrar from which the domain name registration was transferred.

9. Policy Modifications. We reserve the right to modify this Policy at any time with the permission of ICANN. We will post our revised

Policy at <URL> at least thirty (30) calendar days before it becomes effective. Unless this Policy has already been invoked by the submission of a complaint to a Provider, in which event the version of the Policy in effect at the time it was invoked will apply to you until the dispute is over, all such changes will be binding upon you with respect to any domain name registration dispute, whether the dispute arose before, on or after the effective date of our change. In the event that you object to a change in this Policy, your sole remedy is to cancel your domain name registration with us, provided that you will not be entitled to a refund of any fees you paid to us. The revised Policy will apply to you until you cancel your domain name registration

You Tube Twitter LinkedIn Flickr Facebook

RSS Feeds Community Wiki ICANN Blog

© 2014 Internet Corporation For Assigned Names and Numbers. Privacy Policy Terms of Service
Cookie Policy

Who We Are

Get Started

Learning

Participate

Groups

Board

President's Corner

Staff

Careers

Newsletter

Contact Us

Offices

Customer Service

Security Team

PGP Keys

Certificate Authority

Registry Liaison

AOC Review

Organizational Reviews

Request a Speaker

For Journalists

Accountability & Transparency

Accountability Mechanisms

Independent Review Process

Request for Reconsideration

Ombudsman

Governance

Documents

Agreements

AOC Review

Annual Report

Financials

Document Disclosure

Planning

Dashboard

RFPs

Litigation

Correspondence

Help

Dispute Resolution

Domain Name Dispute Resolution

Name Collision

Registrar Problems

WHOIS

EXHIBIT 6

English (/translations) العربية (/ar)

Español (/es) Français (/fr) Русский (/ru)

中文 (/zh)

Log In (/users/sign_in) Sign Up (/users/sign_up)

Search ICANN.org

ICANN (/)

GET STARTED (/GET-STARTED) NEWS & MEDIA (/NEWS) POLICY (/POLICY)

PUBLIC COMMENT (/PUBLIC-COMMENTS) RESOURCES (/RESOURCES)

COMMUNITY (/COMMUNITY) IANA STEWARDSHIP & ACCOUNTABILITY (/STEWARDSHIP-ACCOUNTABILITY)

Resources

- About ICANN (Internet Corporation for Assigned Names and Numbers) (/resources/pages/welcome-2012-02-25-en)
- Board (/resources/pages/board-of-directors-2014-03-19-en)
- Accountability

Rules for Uniform Domain Name (Domain Name) Dispute Resolution Policy (the "Rules")

This page is available in:

(/resources /accountability)

- Governance (/resources /pages /governance-2012-02-25-en)
- Groups (/resources /pages/groups-2012-02-06-en)

Business (/resources /pages /business)

- Contractual Compliance (/resources /pages /compliance-2012-02-25-en)
- Registrars (/resources /pages /registrars-0d-2012-02-25-en)
- Registries (/resources /pages /registries-46-2012-02-25-en)

Operational Metrics (/resources /pages /metrics-gdd-2015-01-30-en)

- Identifier

English | العربية (http://www.icann.org/resources/pages/udrp-rules-2015-03-12-ar) | Español (http://www.icann.org/resources/pages/udrp-rules-2015-03-12-es) | Français (http://www.icann.org/resources/pages/udrp-rules-2015-03-12-fr) | 日本語 (http://www.icann.org/resources/pages/udrp-rules-2015-03-12-ja) | 한국어 (http://www.icann.org/resources/pages/udrp-rules-2015-03-12-ko) | Português (http://www.icann.org/resources/pages/udrp-rules-2015-03-13-pt) | Русский (http://www.icann.org/resources/pages/udrp-rules-2015-03-12-ru) | 中文 (http://www.icann.org/resources/pages/udrp-rules-2015-03-12-zh)

As approved by the ICANN (Internet Corporation for Assigned Names and Numbers) Board of Directors on 28 September 2013 (/resources /board-material/resolutions-2013-09-28-en#1.c).

These Rules are in effect for all UDRP (Uniform Domain-Name Dispute Resolution Policy) proceedings in which a complaint is submitted to a provider on or after 31 July 2015. The prior version of the Rules, applicable to all proceedings in which a complaint was submitted to a Provider on or before 30 July 2015, is at https://www.icann.org/resources/pages/rules-be-2012-02-25-en (/resources/pages/rules-be-2012-02-25-en). UDRP (Uniform Domain-Name Dispute Resolution Policy) Providers may elect to adopt the notice procedures set forth in these Rules prior to 31 July 2015.

Administrative proceedings for the resolution of disputes under the Uniform Dispute Resolution Policy adopted by ICANN (Internet Corporation for Assigned Names and Numbers) shall be governed by these Rules and also the Supplemental Rules of the Provider administering the proceedings, as posted on its web site. To the extent that the Supplemental Rules of any Provider conflict with these Rules, these Rules supersede.

1. Definitions

Systems Security, Stability (Security, Stability and Resiliency) and Resiliency (IS-SSR) (/resources/pages/is-ssr-2014-11-24-en)

- ccTLDs (/resources/pages/cctlds-21-2012-02-25-en)
- Internationalized Domain Names (/resources/pages/idn-2012-02-25-en)
- Universal Acceptance Initiative (/resources/pages/universal-acceptance-2012-02-25-en)
- Policy (/resources/pages/policy-01-2012-02-25-en)
- Public Comment (/public-comments)
- Technical Functions (/resources

In these Rules:

Complainant means the party initiating a complaint concerning a domain-name registration.

ICANN (Internet Corporation for Assigned Names and Numbers) refers to the Internet Corporation for Assigned Names and Numbers.

Lock means a set of measures that a registrar applies to a domain name, which prevents at a minimum any modification to the registrant and registrar information by the Respondent, but does not affect the resolution of the domain name or the renewal of the domain name.

Mutual Jurisdiction means a court jurisdiction at the location of either (a) the principal office of the Registrar (provided the domain-name holder has submitted in its Registration Agreement to that jurisdiction for court adjudication of disputes concerning or arising from the use of the domain name) or (b) the domain-name holder's address as shown for the registration of the domain name in Registrar's Whois database at the time the complaint is submitted to the Provider.

Panel means an administrative panel appointed by a Provider to decide a complaint concerning a domain-name registration.

Panelist means an individual appointed by a Provider to be a member of a Panel.

Party means a Complainant or a Respondent.

Pendency means the time period from the moment a UDRP (Uniform Domain-Name Dispute Resolution Policy) complaint has been submitted by the Complainant to the UDRP (Uniform Domain-Name Dispute Resolution Policy) Provider to the time the UDRP (Uniform Domain-Name Dispute Resolution Policy) decision has been

/pages
/technical-
functions-
2015-10-15-en)

- Contact
(/resources
/pages
/contact-
2012-02-06-en)
- Help
(/resources
/pages/help-
2012-02-03-en)

implemented or the UDRP (Uniform Domain-Name Dispute Resolution Policy) complaint has been terminated.

Policy means the Uniform Domain Name (Domain Name) Dispute Resolution Policy (/en/dndr/udrp/policy.htm) that is incorporated by reference and made a part of the Registration Agreement.

Provider means a dispute-resolution service provider approved by ICANN (Internet Corporation for Assigned Names and Numbers). A list of such Providers appears at http://www.icann.org/en/dndr/udrp/approved-providers.htm (/en/dndr/udrp/approved-providers.htm).

Registrar means the entity with which the Respondent has registered a domain name that is the subject of a complaint.

Registration Agreement means the agreement between a Registrar and a domain-name holder.

Respondent means the holder of a domain-name registration against which a complaint is initiated.

Reverse Domain Name (Domain Name) Hijacking means using the Policy in bad faith to attempt to deprive a registered domain-name holder of a domain name.

Supplemental Rules means the rules adopted by the Provider administering a proceeding to supplement these Rules. Supplemental Rules shall not be inconsistent with the Policy or these Rules and shall cover such topics as fees, word and page limits and guidelines, file size and format modalities, the means for communicating with the Provider and the Panel, and the form of cover sheets.

Written Notice means hardcopy notification by the Provider to the Respondent of the commencement of an administrative proceeding under the Policy which shall

inform the respondent that a complaint has been filed against it, and which shall state that the Provider has electronically transmitted the complaint including any annexes to the Respondent by the means specified herein. Written notice does not include a hardcopy of the complaint itself or of any annexes.

2. Communications

(a) When forwarding a complaint, including any annexes, electronically to the Respondent, it shall be the Provider's responsibility to employ reasonably available means calculated to achieve actual notice to Respondent. Achieving actual notice, or employing the following measures to do so, shall discharge this responsibility:

(i) sending Written Notice of the complaint to all postal-mail and facsimile addresses (A) shown in the domain name's registration data in Registrar's Whois database for the registered domain-name holder, the technical contact, and the administrative contact and (B) supplied by Registrar to the Provider for the registration's billing contact; and

(ii) sending the complaint, including any annexes, in electronic form by e-mail to:

(A) the e-mail addresses for those technical, administrative, and billing contacts;

(B) postmaster@<the contested domain name>; and

(C) if the domain name (or "www." followed by the domain name) resolves to an active web page (other than a generic page the Provider concludes is maintained by a registrar or ISP (Internet Service Provider) for parking domain-names registered by multiple

domain-name holders), any e- mail address shown or e-mail links on that web page; and

(iii) sending the complaint, including any annexes, to any e-mail address the Respondent has notified the Provider it prefers and, to the extent practicable, to all other e-mail addresses provided to the Provider by Complainant under Paragraph 3(b)(v) (/en/help/dndr/udrp/rules#3bv).

(b) Except as provided in Paragraph 2(a) (/en/help/dndr/udrp/rules#2a), any written communication to Complainant or Respondent provided for under these Rules shall be made electronically via the Internet (a record of its transmission being available), or by any reasonably requested preferred means stated by the Complainant or Respondent, respectively (see Paragraphs 3(b)(iii) (/en/help/dndr/udrp/rules#3biii) and 5(b)(iii) (/en/help/dndr/udrp/rules#5biii)).

(c) Any communication to the Provider or the Panel shall be made by the means and in the manner (including, where applicable, the number of copies) stated in the Provider's Supplemental Rules.

(d) Communications shall be made in the language prescribed in Paragraph 11 (/en/help/dndr/udrp/rules#11).

(e) Either Party may update its contact details by notifying the Provider and the Registrar.

(f) Except as otherwise provided in these Rules, or decided by a Panel, all communications provided for under these Rules shall be deemed to have been made:

(i) if via the Internet, on the date that the communication was transmitted, provided that the date of transmission is verifiable; or, where applicable

(ii) if delivered by telecopy or facsimile transmission, on the date shown on the confirmation of transmission; or:

(iii) if by postal or courier service, on the date marked on the receipt.

(g) Except as otherwise provided in these Rules, all time periods calculated under these Rules to begin when a communication is made shall begin to run on the earliest date that the communication is deemed to have been made in accordance with Paragraph 2(f) (/en/help/dndr/udrp/rules#2f).

(h) Any communication by

(i) a Panel to any Party shall be copied to the Provider and to the other Party;

(ii) the Provider to any Party shall be copied to the other Party; and

(iii) a Party shall be copied to the other Party, the Panel and the Provider, as the case may be.

(i) It shall be the responsibility of the sender to retain records of the fact and circumstances of sending, which shall be available for inspection by affected parties and for reporting purposes. This includes the Provider in sending Written Notice to the Respondent by post and/or facsimile under Paragraph 2(a)(i).

(j) In the event a Party sending a communication receives notification of non-delivery of the communication, the Party shall promptly notify the Panel (or, if no Panel is yet appointed, the Provider) of the circumstances of the notification. Further proceedings concerning the communication and any response shall be as directed by the Panel (or the Provider).

3. The Complaint

(a) Any person or entity may initiate an administrative proceeding by submitting a complaint in accordance with the Policy and these Rules to any Provider approved by ICANN (Internet Corporation for Assigned Names and Numbers). (Due to capacity constraints or for other reasons, a Provider's ability to accept complaints may be suspended at times. In that event, the Provider shall refuse the submission. The person or entity may submit the complaint to another Provider.)

(b) The complaint including any annexes shall be submitted in electronic form and shall:

(i) Request that the complaint be submitted for decision in accordance with the Policy and these Rules;

(ii) Provide the name, postal and e-mail addresses, and the telephone and telefax numbers of the Complainant and of any representative authorized to act for the Complainant in the administrative proceeding;

(iii) Specify a preferred method for communications directed to the Complainant in the administrative proceeding (including person to be contacted, medium, and address information) for each of (A) electronic-only material and (B) material including hard copy (where applicable);

(iv) Designate whether Complainant elects to have the dispute decided by a single-member or a three-member Panel and, in the event Complainant elects a three-member Panel, provide the names and contact details of three candidates to serve as one of the Panelists (these candidates may be drawn from any ICANN (Internet Corporation for

Assigned Names and Numbers)-approved Provider's list of panelists);

(v) Provide the name of the Respondent (domain-name holder) and all information (including any postal and e-mail addresses and telephone and telefax numbers) known to Complainant regarding how to contact Respondent or any representative of Respondent, including contact information based on pre-complaint dealings, in sufficient detail to allow the Provider to send the complaint as described in Paragraph 2(a) (/en/help/dndr/udrp/rules#2a);

(vi) Specify the domain name(s) that is/are the subject of the complaint;

(vii) Identify the Registrar(s) with whom the domain name(s) is/are registered at the time the complaint is filed;

(viii) Specify the trademark(s) or service mark(s) on which the complaint is based and, for each mark, describe the goods or services, if any, with which the mark is used (Complainant may also separately describe other goods and services with which it intends, at the time the complaint is submitted, to use the mark in the future.);

(ix) Describe, in accordance with the Policy, the grounds on which the complaint is made including, in particular,

(1) the manner in which the domain name(s) is/are identical or confusingly similar to a trademark or service mark in which the Complainant has rights; and

(2) why the Respondent (domain-name holder) should be considered as having no

rights or legitimate interests in respect of the domain name(s) that is/are the subject of the complaint; and

(3) why the domain name(s) should be considered as having been registered and being used in bad faith

(The description should, for elements (2) and (3), discuss any aspects of Paragraphs 4(b) (/en/dndr/udrp/policy.htm#4b) and 4(c) (/en/dndr/udrp/policy.htm#4c) of the Policy that are applicable. The description shall comply with any word or page limit set forth in the Provider's Supplemental Rules.);

(x) Specify, in accordance with the Policy, the remedies sought;

(xi) Identify any other legal proceedings that have been commenced or terminated in connection with or relating to any of the domain name(s) that are the subject of the complaint;

(xii) State that Complainant will submit, with respect to any challenges to a decision in the administrative proceeding canceling or transferring the domain name, to the jurisdiction of the courts in at least one specified Mutual Jurisdiction;

(xiii) Conclude with the following statement followed by the signature (in any electronic format) of the Complainant or its authorized representative:

"Complainant agrees that its claims and remedies concerning the registration of the domain name, the dispute, or the dispute's resolution shall be solely against the domain-name holder and waives all such claims and remedies against (a) the dispute-

resolution provider and panelists, except in the case of deliberate wrongdoing, (b) the registrar, (c) the registry administrator, and (d) the Internet Corporation for Assigned Names and Numbers, as well as their directors, officers, employees, and agents."

"Complainant certifies that the information contained in this Complaint is to the best of Complainant's knowledge complete and accurate, that this Complaint is not being presented for any improper purpose, such as to harass, and that the assertions in this Complaint are warranted under these Rules and under applicable law, as it now exists or as it may be extended by a good-faith and reasonable argument."; and

(xiv) Annex any documentary or other evidence, including a copy of the Policy applicable to the domain name(s) in dispute and any trademark or service mark registration upon which the complaint relies, together with a schedule indexing such evidence.

(c) The complaint may relate to more than one domain name, provided that the domain names are registered by the same domain-name holder.

4. Notification of Complaint

(a) The Provider shall submit a verification request to the Registrar. The verification request will include a request to Lock the domain name.

(b) Within two (2) business days of receiving the Provider's verification request, the Registrar shall provide the information requested in the verification request and confirm that a Lock of the domain name has been

applied. The Registrar shall not notify the Respondent of the proceeding until the Lock status has been applied. The Lock shall remain in place through the remaining Pendency of the UDRP (Uniform Domain-Name Dispute Resolution Policy) proceeding. Any updates to the Respondent's data, such as through the result of a request by a privacy or proxy provider to reveal the underlying customer data, must be made before the two (2) business day period concludes or before the Registrar verifies the information requested and confirms the Lock to the UDRP (Uniform Domain-Name Dispute Resolution Policy) Provider, whichever occurs first. Any modification(s) of the Respondent's data following the two (2) business day period may be addressed by the Panel in its decision.

(c) The Provider shall review the complaint for administrative compliance with the Policy and these Rules and, if in compliance, shall forward the complaint, including any annexes, electronically to the Respondent and Registrar and shall send Written Notice of the complaint (together with the explanatory cover sheet prescribed by the Provider's Supplemental Rules) to the Respondent, in the manner prescribed by Paragraph 2(a) (/en/help/dndr/udrp/rules#2a), within three (3) calendar days following receipt of the fees to be paid by the Complainant in accordance with Paragraph 19 (/en/help /dndr/udrp/rules#19).

(d) If the Provider finds the complaint to be administratively deficient, it shall promptly notify the Complainant and the Respondent of the nature of the deficiencies identified. The Complainant shall have five (5) calendar days within which to correct any such deficiencies, after which the administrative proceeding will be deemed withdrawn without prejudice to submission of a different complaint by Complainant.

(e) If the Provider dismisses the complaint due to an administrative deficiency, or the Complainant voluntarily

withdraws its complaint, the Provider shall inform the Registrar that the proceedings have been withdrawn, and the Registrar shall release the Lock within one (1) business day of receiving the dismissal or withdrawal notice from the Provider.

(f) The date of commencement of the administrative proceeding shall be the date on which the Provider completes its responsibilities under Paragraph 2(a) (/en/help/dndr/udrp/rules#2a) in connection with sending the complaint to the Respondent.

(g) The Provider shall immediately notify the Complainant, the Respondent, the concerned Registrar(s), and ICANN (Internet Corporation for Assigned Names and Numbers) of the date of commencement of the administrative proceeding. The Provider shall inform the Respondent that any corrections to the Respondent's contact information during the remaining Pendency of the UDRP (Uniform Domain-Name Dispute Resolution Policy) proceedings shall be communicated to the Provider further to Rule 5(c)(ii) and 5(c)(iii).

5. The Response

(a) Within twenty (20) days of the date of commencement of the administrative proceeding the Respondent shall submit a response to the Provider.

(b) The Respondent may expressly request an additional four (4) calendar days in which to respond to the complaint, and the Provider shall automatically grant the extension and notify the Parties thereof. This extension does not preclude any additional extensions that may be given further to 5(d) of the Rules.

(c) The response, including any annexes, shall be submitted in electronic form and shall:

(i) Respond specifically to the statements and allegations contained in the complaint and include any and all bases for the Respondent (domain-name holder) to retain registration and use of the disputed domain name (This portion of the response shall comply with any word or page limit set forth in the Provider's Supplemental Rules.);

(ii) Provide the name, postal and e-mail addresses, and the telephone and telefax numbers of the Respondent (domain-name holder) and of any representative authorized to act for the Respondent in the administrative proceeding;

(iii) Specify a preferred method for communications directed to the Respondent in the administrative proceeding (including person to be contacted, medium, and address information) for each of (A) electronic-only material and (B) material including hard copy (where applicable);

(iv) If Complainant has elected a single-member panel in the complaint (see Paragraph 3(b)(iv) (/en/help/dndr/udrp/rules#3biv)), state whether Respondent elects instead to have the dispute decided by a three-member panel;

(v) If either Complainant or Respondent elects a three-member Panel, provide the names and contact details of three candidates to serve as one of the Panelists (these candidates may be drawn from any ICANN (Internet Corporation for Assigned Names and Numbers)-approved Provider's list of panelists);

(vi) Identify any other legal proceedings that have been commenced or terminated in connection with or relating to any of the domain name(s) that are the subject of the complaint;

(vii) State that a copy of the response including any annexes has been sent or transmitted to the Complainant, in accordance with Paragraph 2(b) (/en/help/dndr/udrp/rules#2b); and

(viii) Conclude with the following statement followed by the signature (in any electronic format) of the Respondent or its authorized representative:

"Respondent certifies that the information contained in this Response is to the best of Respondent's knowledge complete and accurate, that this Response is not being presented for any improper purpose, such as to harass, and that the assertions in this Response are warranted under these Rules and under applicable law, as it now exists or as it may be extended by a good-faith and reasonable argument."; and

(ix) Annex any documentary or other evidence upon which the Respondent relies, together with a schedule indexing such documents.

(d) If Complainant has elected to have the dispute decided by a single-member Panel and Respondent elects a three-member Panel, Respondent shall be required to pay one-half of the applicable fee for a three-member Panel as set forth in the Provider's Supplemental Rules. This payment shall be made together with the submission of the response to the Provider. In the event that the required payment is not made, the dispute shall be decided by a single-member Panel.

(e) At the request of the Respondent, the Provider may, in exceptional cases, extend the period of time for the filing of the response. The period may also be extended by written stipulation between the Parties, provided the stipulation is approved by the Provider.

(f) If a Respondent does not submit a response, in the absence of exceptional circumstances, the Panel shall decide the dispute based upon the complaint.

6. Appointment of the Panel and Timing of Decision

(a) Each Provider shall maintain and publish a publicly available list of panelists and their qualifications.

(b) If neither the Complainant nor the Respondent has elected a three-member Panel (Paragraphs 3(b)(iv) (/en/help/dndr/udrp/rules#3biv) and 5(b)(iv) (/en/help /dndr/udrp/rules#5biv)), the Provider shall appoint, within five (5) calendar days following receipt of the response by the Provider, or the lapse of the time period for the submission thereof, a single Panelist from its list of panelists. The fees for a single-member Panel shall be paid entirely by the Complainant.

(c) If either the Complainant or the Respondent elects to have the dispute decided by a three-member Panel, the Provider shall appoint three Panelists in accordance with the procedures identified in Paragraph 6(e) (/en/help /dndr/udrp/rules#6e). The fees for a three-member Panel shall be paid in their entirety by the Complainant, except where the election for a three-member Panel was made by the Respondent, in which case the applicable fees shall be shared equally between the Parties.

(d) Unless it has already elected a three-member Panel, the Complainant shall submit to the Provider, within five (5) calendar days of communication of a response in which the Respondent elects a three-member Panel, the names and contact details of three candidates to serve as one of the Panelists. These candidates may be drawn from any ICANN (Internet Corporation for Assigned Names and Numbers)-approved Provider's list of panelists.

(e) In the event that either the Complainant or the Respondent elects a three-member Panel, the Provider shall endeavor to appoint one Panelist from the list of candidates provided by each of the Complainant and the Respondent. In the event the Provider is unable within five (5) calendar days to secure the appointment of a Panelist on its customary terms from either Party's list of candidates, the Provider shall make that appointment from its list of panelists. The third Panelist shall be appointed by the Provider from a list of five candidates submitted by the Provider to the Parties, the Provider's selection from among the five being made in a manner that reasonably balances the preferences of both Parties, as they may specify to the Provider within five (5) calendar days of the Provider's submission of the five-candidate list to the Parties.

(f) Once the entire Panel is appointed, the Provider shall notify the Parties of the Panelists appointed and the date by which, absent exceptional circumstances, the Panel shall forward its decision on the complaint to the Provider.

7. Impartiality and Independence

A Panelist shall be impartial and independent and shall have, before accepting appointment, disclosed to the Provider any circumstances giving rise to justifiable doubt as to the Panelist's impartiality or independence. If, at any stage during the administrative proceeding, new circumstances arise that could give rise to justifiable doubt as to the impartiality or independence of the Panelist, that Panelist shall promptly disclose such circumstances to the Provider. In such event, the Provider shall have the discretion to appoint a substitute Panelist.

8. Communication Between Parties and the Panel

No Party or anyone acting on its behalf may have any unilateral communication with the Panel. All communications between a Party and the Panel or the Provider shall be made to a case

administrator appointed by the Provider in the manner prescribed in the Provider's Supplemental Rules.

9. Transmission of the File to the Panel

The Provider shall forward the file to the Panel as soon as the Panelist is appointed in the case of a Panel consisting of a single member, or as soon as the last Panelist is appointed in the case of a three-member Panel.

10. General Powers of the Panel

(a) The Panel shall conduct the administrative proceeding in such manner as it considers appropriate in accordance with the Policy and these Rules.

(b) In all cases, the Panel shall ensure that the Parties are treated with equality and that each Party is given a fair opportunity to present its case.

(c) The Panel shall ensure that the administrative proceeding takes place with due expedition. It may, at the request of a Party or on its own motion, extend, in exceptional cases, a period of time fixed by these Rules or by the Panel.

(d) The Panel shall determine the admissibility, relevance, materiality and weight of the evidence.

(e) A Panel shall decide a request by a Party to consolidate multiple domain name disputes in accordance with the Policy and these Rules.

11. Language of Proceedings

(a) Unless otherwise agreed by the Parties, or specified otherwise in the Registration Agreement, the language of the administrative proceeding shall be the language of the Registration Agreement, subject to the authority of the

Panel to determine otherwise, having regard to the circumstances of the administrative proceeding.

(b) The Panel may order that any documents submitted in languages other than the language of the administrative proceeding be accompanied by a translation in whole or in part into the language of the administrative proceeding.

12. Further Statements

In addition to the complaint and the response, the Panel may request, in its sole discretion, further statements or documents from either of the Parties.

13. In-Person Hearings

There shall be no in-person hearings (including hearings by teleconference, videoconference, and web conference), unless the Panel determines, in its sole discretion and as an exceptional matter, that such a hearing is necessary for deciding the complaint.

14. Default

(a) In the event that a Party, in the absence of exceptional circumstances, does not comply with any of the time periods established by these Rules or the Panel, the Panel shall proceed to a decision on the complaint.

(b) If a Party, in the absence of exceptional circumstances, does not comply with any provision of, or requirement under, these Rules or any request from the Panel, the Panel shall draw such inferences therefrom as it considers appropriate.

15. Panel Decisions

(a) A Panel shall decide a complaint on the basis of the statements and documents submitted and in accordance

with the Policy, these Rules and any rules and principles of law that it deems applicable.

(b) In the absence of exceptional circumstances, the Panel shall forward its decision on the complaint to the Provider within fourteen (14) days of its appointment pursuant to Paragraph 6 (/en/help/dndr/udrp/rules#6).

(c) In the case of a three-member Panel, the Panel's decision shall be made by a majority.

(d) The Panel's decision shall be in writing, provide the reasons on which it is based, indicate the date on which it was rendered and identify the name(s) of the Panelist(s).

(e) Panel decisions and dissenting opinions shall normally comply with the guidelines as to length set forth in the Provider's Supplemental Rules. Any dissenting opinion shall accompany the majority decision. If the Panel concludes that the dispute is not within the scope of Paragraph 4(a) (/en/dndr/udrp/policy.htm#4a) of the Policy, it shall so state. If after considering the submissions the Panel finds that the complaint was brought in bad faith, for example in an attempt at Reverse Domain Name (Domain Name) Hijacking or was brought primarily to harass the domain-name holder, the Panel shall declare in its decision that the complaint was brought in bad faith and constitutes an abuse of the administrative proceeding.

16. Communication of Decision to Parties

(a) Within three (3) business days after receiving the decision from the Panel, the Provider shall communicate the full text of the decision to each Party, the concerned Registrar(s), and ICANN (Internet Corporation for Assigned Names and Numbers). The concerned Registrar(s) shall within three (3) business days of receiving the decision from the Provider communicate to

each Party, the Provider, and ICANN (Internet Corporation for Assigned Names and Numbers) the date for the implementation of the decision in accordance with the Policy.

(b) Except if the Panel determines otherwise (see Paragraph 4(j) (/en/dndr/udrp/policy.htm#4j) of the Policy), the Provider shall publish the full decision and the date of its implementation on a publicly accessible web site. In any event, the portion of any decision determining a complaint to have been brought in bad faith (see Paragraph 15(e) (/en/help/dndr/udrp/rules#15e) of these Rules) shall be published.

17. Settlement or Other Grounds for Termination

(a) If, before the Panel's decision, the Parties agree on a settlement, the Panel shall terminate the administrative proceeding. A settlement shall follow steps 17(a)(i) – 17(a)(vii):

(i) The Parties provide written notice of a request to suspend the proceedings because the parties are discussing settlement to the Provider.

(ii) The Provider acknowledges receipt of the request for suspension and informs the Registrar of the suspension request and the expected duration of the suspension.

(iii) The Parties reach a settlement and provide a standard settlement form to the Provider further to the Provider's supplemental rules and settlement form. The standard settlement form is not intended to be an agreement itself, but only to summarize the essential terms of the Parties' separate settlement agreement. The Provider shall not disclose the completed standard settlement form to any third party.

(iv) The Provider shall confirm to the Registrar, copying the Parties, the outcome of the settlement as it relates to actions that need to be taken by the Registrar.

(v) Upon receiving notice from the Provider further to 17(a)(iv), the Registrar shall remove the Lock within two (2) business days.

(vi) The Complainant shall confirm to the Provider that the settlement as it relates to the domain name(s) has been implemented further to the Provider's supplemental rules.

(vii) The Provider will dismiss the proceedings without prejudice unless otherwise stipulated in the settlement.

(b) If, before the Panel's decision is made, it becomes unnecessary or impossible to continue the administrative proceeding for any reason, the Panel shall terminate the administrative proceeding, unless a Party raises justifiable grounds for objection within a period of time to be determined by the Panel.

18. Effect of Court Proceedings

(a) In the event of any legal proceedings initiated prior to or during an administrative proceeding in respect of a domain-name dispute that is the subject of the complaint, the Panel shall have the discretion to decide whether to suspend or terminate the administrative proceeding, or to proceed to a decision.

(b) In the event that a Party initiates any legal proceedings during the Pendency of an administrative proceeding in respect of a domain-name dispute that is the subject of the complaint, it shall promptly notify the Panel and the Provider. See Paragraph 8 (/en/help

/dndr/udrp/rules#8) above.

19. Fees

(a) The Complainant shall pay to the Provider an initial fixed fee, in accordance with the Provider's Supplemental Rules, within the time and in the amount required. A Respondent electing under Paragraph 5(b)(iv) (/en/help/dndr/udrp/rules#5biv) to have the dispute decided by a three-member Panel, rather than the single-member Panel elected by the Complainant, shall pay the Provider one-half the fixed fee for a three-member Panel. See Paragraph 5(c) (/en/help/dndr/udrp/rules#5c). In all other cases, the Complainant shall bear all of the Provider's fees, except as prescribed under Paragraph 19(d) (/en/help/dndr/udrp/rules#19d). Upon appointment of the Panel, the Provider shall refund the appropriate portion, if any, of the initial fee to the Complainant, as specified in the Provider's Supplemental Rules.

(b) No action shall be taken by the Provider on a complaint until it has received from Complainant the initial fee in accordance with Paragraph 19(a) (/en/help/dndr/udrp/rules#19a).

(c) If the Provider has not received the fee within ten (10) calendar days of receiving the complaint, the complaint shall be deemed withdrawn and the administrative proceeding terminated.

(d) In exceptional circumstances, for example in the event an in-person hearing is held, the Provider shall request the Parties for the payment of additional fees, which shall be established in agreement with the Parties and the Panel.

20. Exclusion of Liability

Except in the case of deliberate wrongdoing, neither the

Provider nor a Panelist shall be liable to a Party for any act or omission in connection with any administrative proceeding under these Rules.

21. Amendments

The version of these Rules in effect at the time of the submission of the complaint to the Provider shall apply to the administrative proceeding commenced thereby. These Rules may not be amended without the express written approval of ICANN (Internet Corporation for Assigned Names and Numbers).

You Tube (http://www.youtube.com/icannnews) Twitter (https://www.twitter.com/icann) LinkedIn (https://www.linkedin.com/company/icann) Flickr (http://www.flickr.com/photos/icann) Facebook (http://www.facebook.com/icannorg)

RSS Feeds (/en/news/rss) Community Wiki (https://community.icann.org) ICANN Blog (/news/blog)

© 2014 Internet Corporation For Assigned Names and Numbers. Privacy Policy (/en/help/privacy) Terms of Service (/en/help/tos) Cookie Policy (/en/help/privacy-cookie-policy)

Who We Are

Get Started (/get-started)

Learning (/en/about/learning)

Participate (/en/about/participate)

Groups (https://www.icann.org/resources/pages/groups-2012-02-06-en)

Board (/resources/pages/board-of-directors-2014-03-19-en)

President's Corner (/presidents-corner)

Staff (/en/about/staff)

Careers (https://icann-openhire.silkroad.com/epostings/index.cfm?fuseaction=app.allpositions&company_id=16029&version=1)

Newsletter (/en/news/newsletter)

Development and Public Responsibility (https://www.icann.org/development-and-public-responsibility)

Contact Us

Offices (https://forms.icann.org/en/contact)

Global Support (/resources/pages/customer-support-2015-06-22-en)

Security Team (/about/staff/security)

PGP Keys (/en/contact/pgp-keys)

Certificate Authority (/contact/certificate-authority)

Registry Liaison (/resources/pages/contact-f2-2012-02-25-en)

AOC Review (http://forms.icann.org/en/about/aoc-review/contact)

Organizational Reviews (http://forms.icann.org/en/groups/reviews/contact)

Request a Speaker (http://forms.icann.org/en/contact/speakers)

For Journalists (/en/news/press)

Accountability & Transparency

Accountability Mechanisms (/en/news/in-focus/accountability/mechanisms)

Independent Review Process (/resources/pages/irp-2012-02-25-en)

Request for Reconsideration (/groups/board/governance/reconsideration)

Ombudsman (/help/ombudsman)

Governance

Documents (/en/about/governance)

Agreements (/en/about/agreements)

AOC Review (/en/about/aoc-review)

Annual Report (/about/annual-report)

Financials (/en/about/financials)

Document Disclosure (/en/about/transparency)

Planning (/en/about/planning)

Dashboard Beta (https://www.icann.org/dashboard)

RFPs (/en/news/rfps)

Litigation (/en/news/litigation)

Correspondence (/en/news/correspondence)

Help

Dispute Resolution (/en/help/dispute-resolution)

Domain Name Dispute Resolution (/en/help/dndr)

Name Collision (/en/help/name-collision)

Registrar Problems (/en/news/announcements/announcement-06mar07-en.htm)

WHOIS (http://whois.icann.org/)

EXHIBIT 7

Terms and Conditions

This Registration Agreement ("Agreement") sets forth the terms and conditions of your use of domain name registration and related services ("Services"). In this Agreement "you" and "your" refer to you and the registrant associated with the WHOIS contact information for the domain name. "We", "us" and "our" refers to NameSilo, LLC.

1. YOUR AGREEMENT: By using the Services, you agree to all terms and conditions of this Agreement, the UDRP (defined below) and any rules, policies, or agreements published in association with specific Services and/or which may be adopted or enforced by the Internet Corporation for Assigned Names and Numbers ("ICANN"), any registry, or governments.
2. CHANGES TO THIS AGREEMENT: This Agreement may change over time, either through amendments by us, changes to ICANN policy or applicable law which may or may not be reflected in the text of this Agreement, or otherwise. Before any material changes to this Agreement become binding on you (other than changes resulting from a change in ICANN policy or applicable law), we will notify you of such changes by, for example, sending email to you at your email address of record, or by posting the changes on our web site. If, as a result of such a change, you no longer agree with the terms of this Agreement, your exclusive remedies are (a) to transfer your domain name registration services to another registrar, or (b) to cancel your domain name registration services with us. Your continued use of the Services following notification of a change in this Agreement indicates your consent to the changes. Unless otherwise specified by us, any such change binds you: (1) 30 days after we notify you of the change, or (2) immediately if such change is a result of a new or amended ICANN policy or applicable law.
3. YOUR ACCOUNT: You must create an account to use the Services ("Account"). You are solely responsible for maintaining, securing, updating, and keeping strictly confidential all login IDs and passwords, and for all access to and use of your Account by you or any third party.

    a. ACCOUNT CONTACT INFORMATION AND DOMAIN NAME WHOIS INFORMATION:

        i. You must provide certain current, complete and accurate information about you with respect to your Account information and with respect to the WHOIS information for your domain name(s). You must maintain and update this information as needed to keep it current, complete and accurate. You must submit the following with respect to you, the administrative, technical, and billing contacts for your domain name registration(s) and other Services: the full name, postal address, e-mail address, voice telephone number, and fax number if available of the Registered Name Holder; name of authorized person for contact purposes in the case of an Registered Name Holder that is an organization, association, or corporation; and the data elements listed in Subsections 3.3.1.2, 3.3.1.7 and 3.3.1.8 of the 2013 ICANN RAA. The type of information you are required to provide may change and you must provide such information and keep your Account information current. Not providing requested information may prevent you from obtaining all Services and you must update any such information within seven (7) days of change.

        ii. You may provide information regarding the name-servers assigned to your domain name(s). If you do not provide complete name-server information, we reserve the right to supply this information (and point your domain name to a website of our choosing) until such time as you elect to supply the name-server information. Any newly registered domain names will default to using our name-servers which will load our default parking page, however, you have the ability to provide new name-server information by logging into your account.

    b. OBLIGATIONS RELATING TO THE ACCOUNT AND WHOIS CONTACT INFORMATION:

        i. If, in obtaining Services, you provide information about or on behalf of a third party, you represent and warrant that you have (a) provided notice to that third party of the disclosure and use of that party's information as set forth in this Agreement, and (b) obtained the third party's express written or verbal consent to the disclosure and use of that party's information as set forth in this Agreement.

        ii. You represent and warrant that the statements in your application are true and that no Services are being procured for any unlawful purpose, including but not limited to the infringement of any intellectual property right, the unauthorized transfer to yourself or any other party of any domain name or Services, or the violation of any laws, rules, or regulations (the"Illegal Uses"). Providing inaccurate information and willful failure to update information within seven (7) days of any change, or failure to respond for over fifteen (15) days to inquiries concerning the accuracy of contact details associated with your registration, failing to immediately update information or engaging in any Illegal Uses will constitute an incurable material breach of this Agreement. Your failure to respond for over three (3) calendar days to inquiries by us concerning the accuracy of Account and WHOIS contact information shall constitute an incurable material breach of this Agreement.

        iii. You are responsible for regularly monitoring email sent to the email address in your Account. You may lose your rights to the domain name(s) or your right to receive the

Feedback On the New Site?

This site uses cookies to provide you with a better user experience. For more information, refer to our Privacy Policy

Confirm

i. In order to change any of your Account or domain name WHOIS information, you must access your Account with us. It is your duty to safeguard your Account login identifier and password from any unauthorized use. Any person in possession of your Account login identifier and password will have both the ability and your authorization to modify your Account and domain name information, initiate transfers of your domain name(s) to other registrars, initiate registrant changes to your domain names which may terminate your rights to use such domain name(s), update DNS changes to your domain name(s) which may result in changes to the content associated with your domain name(s) and take other actions which may affect or terminate your rights and access to your domain name(s) and/or the Services.

ii. We will take reasonable precautions to protect the information we obtain from you from loss, misuse, unauthorized access or disclosure, alteration or destruction of that information and such reasonable precautions include procedures for releasing Account access information to parties who claim to have lost Account access information. If we take reasonable precautions in relation thereto, IN NO EVENT SHALL WE BE LIABLE IF SUCH REASONABLE PRECAUTIONS DO NOT PREVENT THE UNAUTHORIZED USE OR MISUSE OF YOUR ACCOUNT IDENTIFIER OR PASSWORD AND, EVEN IF WE FAIL TO TAKE REASONABLE PRECAUTIONS, OUR LIABILITY UNDER ANY CIRCUMSTANCES SHALL BE LIMITED BY THE LIMITATION OF LIABILITY PROVISION FOUND IN PARAGRAPH 13 BELOW IN THIS AGREEMENT.

iii. If you contact us alleging that a third party has unauthorized access to your Account or domain names, we may charge you administrative fees, currently set at $100 (US dollars) per hour, for our time spent in relation to the matter, regardless of whether or not we return control over the Account and/or domain name(s) to you. You will indemnify us for any reasonable attorneys' fees and costs we may incur in relation to the matter, even if those fees and costs accrue as a result of defending an action, or responding to a threat of an action, initiated by You or a third party.

iv. You have the ability to create Sub-User accounts as well. These Sub-User accounts allow the people you designate to access certain functionality, including those listed in section c(i) above. You have the option of configuring each Sub-User account to have access to any stored payment profiles as well as to set an expiration date representing the revocation of that Sub-User's ability to access your account. You are entirely responsible for any changes requested or made by any Sub-Users you create, and in no event will we be responsible for any undesirable impact to you as a result of any such changes.

v. You are responsible for ensuring your beneficiaries have appropriate access to your NameSilo account(s) in the event of your death or disability. We strongly encourage all account holders to treat their domains like other important assets and to therefore implement a plan of succession upon their inability to access their account. Failure to make the necessary provisions to ensure your beneficiaries have access to your applicable NameSilo account(s) before your death or disability may make accessing your account (including, but not limited to, account funds balance, domain names and sale proceeds) impossible. Please be sure to also consider optional account security usage such as 2-Factor Authentication and Domain Defender. It is also very important that your account information match documentation we may receive in the event of your death such as a death certificate. While we may attempt to work with your beneficiaries to gain access to your account and associated account assets, this is at our sole discretion. It is very difficult in many cases to prove important issues concerning the rightful access to accounts by beneficiaries, and our first priority is the privacy and security of our account holders. In the event we are able to work with a beneficiary to grant account access, we reserve the right to lock domains for a period of time to be solely determined by us. This lock may include, among other things, preventing changes, preventing transfer to a different registrar and preventing transfer to a different account.

d. SHARING OF WHOIS INFORMATION:

I. We will make available the domain name registration information you provide or that we otherwise maintain to the following parties: ICANN, any ICANN-authorized escrow service, the registry administrator(s), and to other third parties as ICANN, registry administrators and applicable laws may require or permit (including through web-based and other on-line WHOIS lookup systems), whether during or after the term of your domain name registration services of the domain name. You irrevocably waive any and all claims and causes of action you may have arising from such disclosure or use of such information. We may make publicly available, or directly available to third parties, some, or all, of the information you provide, for purposes of inspection (such as through our WHOIS service) or for targeted marketing and other purposes as required or permitted by applicable laws, including by way of bulk WHOIS data access provided to third parties who enter into a bulk WHOIS data access agreement with us. We reserve the right to discontinue providing bulk WHOIS data access to third parties.

II. ICANN may establish or modify the guidelines, limits and/or requirements that relate to the amount and type of information that we may or must make available to the public or to private entities, and the manner in which such information is made available. Information regarding ICANN's guidelines and requirements regarding WHOIS can be found at http://www.icann.org/registrars/wmrp.htm, http://www.icann.org/registrars/wdrp.htm, and elsewhere on the ICANN website at http://www.icann.org/.

III. You consent to the data processing referred to above.

Feedback On the New Site?

This site uses cookies to provide you with a better user experience. For more information, refer to our Privacy Policy

Confirm

4. OUR SERVICES:

a. DOMAIN NAME REGISTRATION.

i. We are accredited registrars with ICANN for generic Top Level Domain Names ("gTLDs") (such as .com, .net, .org, etc.). ICANN oversees registrations and other aspects of the gTLDs. Domain name registrations are not effective until the registry administrator puts them into effect. Domain name registrations are only for limited terms which end on the expiration date. For domain names which are created as a new registration out of the pool of available domain names, the term begins on the date the domain name registration is acknowledged by the applicable registry. For domain name registrations which were not returned to the pool of available domain names, the term begins on the date the previous registrant's domain name registration was acknowledged by the applicable registry.

ii. We are not liable or responsible in any way for any errors, omissions or any other actions by the registry administrator arising out of or related to a request to register, renew, modify the settings for, or transfer of a domain name registration. You acknowledge that domain name registration is a service, domain name registrations do not exist independently from services provided pursuant to this or a similar registration agreement with a registrar, domain name registration services do not create a property interest and you have no such property interest in any domain name(s) which you may register with us.

b. NOT INCLUDED IN THE DOMAIN NAME REGISTRATION SERVICES:

i. We are not responsible to determine whether the domain name(s) you select, or the use you or others make of the domain name(s), or other use of the Services, infringes legal rights of others. It is your responsibility to know whether or not the domain name(s) you select or use or allow others to use infringe legal rights of others.

ii. We might be ordered by a court or arbitrator to cancel, modify, or transfer your domain name; it is your responsibility to list accurate contact information in association with your Account and to communicate with litigants, potential litigants, and governmental authorities. It is not our responsibility to forward court orders or other communications to you. Our policy is to comply with court orders from courts of competent jurisdiction as well as UDRP Panel decisions. If you contact us informing us that you are contesting a court order from a court of competent jurisdiction, we may, but are not obligated to, place a transfer lock on the domain name pending the outcome of the dispute. If you contact us informing us that you are contesting an adverse UDRP Panel decision, your time limits and procedures to do so are subject to the requirements set forth in the UDRP. We may, but are not obligated to, delay implementation of a UDRP Panel decision based solely on your informing us that you intend to contest the decision.

c. WHOIS PRIVACY: We offer a privacy service which substitutes your information with our default information within WHOIS. In the event that you select to utilize this WHOIS Privacy service for one or more of your domains, the following applies:

i. The information you submit related to the various domain roles (registrant, administrative, technical and billing) will remain associated with the domain at all times. We make no claims to the ownership or management of your domains when selecting to use our WHOIS Privacy service.

ii. The terms of this Agreement related to your responsibilities to maintain the accuracy of your contact information are not altered or waived due to your use of this service.

iii. We will provide information to WHOIS at our discretion which will hide your information. This information may reference a WHOIS privacy service other than our name.

iv. You authorize us, or the party referenced in the WHOIS record for your domains utilizing this service, to discard any and all postal mail and electronic mail addressed to the address provided in WHOIS. We are not responsible for forwarding any correspondence directed to your domain names. We will provide a mechanism for entities to make contact with you via a web page that will be referenced in the private WHOIS records. It is entirely at our discretion to forward none, some or all of the correspondence directed to you. We also provide a mechanism for you to enter the email address you would like to use to receive email addressed to the email address in WHOIS for your private domains. We will use our best efforts to forward any such email to the address you provide, but we make no guarantee that we will be able to do so. You agree to provide an email address that complies with the rest of our terms or terms imposed by ICANN or the respective domain registries.

v. You represent and warrant that your use of the WHOIS privacy service will be in good faith and that none of the content found on any web sites or IP addresses associated with domains utilizing the WHOIS privacy service infringes upon the legal rights of any third-party (including, but not limited to, any third-party's trademark, trade name or copyrighted material), and that none of the content is, or is connected to, terrorism, impersonation of a third-party, illegal activities or the transmission of spam, viruses, trojan horses or any other harmful routine or data.

vi. WHOIS privacy is not available for .us domains.

vii. The "AGENTS AND LICENSES" policies covered below also apply to your use of WHOIS Privacy.

viii. We reserve the right in our sole judgment to suspend, terminate and/or disclose your

Feedback On the New Site?

This site uses cookies to provide you with a better user experience. For more information, refer to our Privacy Policy

Confirm

b. If necessary to comply with applicable laws, subpoenas, court orders, a UDRP action or action initiated by any other entity with appropriate jurisdiction

c. If we deem that continuing to provide WHOIS privacy services places us in any jeopardy of of harm including financial loss or legal liability on our behalf or on the behalf of any of our partners, affiliates, employees or managers

d. If we believe you have not completely abided by your representations and warranties listed in this Agreement

ix. In the event that we or a third-party believe you to be infringing upon any part of this Agreement, we will contact you at the email address associated with your account. It is your responsibility to reply to any such communication within three (3) days. We are not responsible for any failure to deliver any such notification as things beyond our control may occur that could prevent delivery. If you fail to reply within the given time frame, or if, in our sole judgment, we believe your reply does not adequately address the points raised in our email, we reserve the right to immediately release your contact information and to suspend or terminate the WHOIS privacy service. This would result in your information being made available via WHOIS. You further agree that we disclaim any liability arising out of undertaking this action and any direct or indirect consequences experienced as a result of releasing your information or suspending or terminating the WHOIS privacy service.

x. In addition to all other indemnity clauses in this Agreement, you agree to defend, release, and indemnify us, ICANN, the registry operators as well as any of our employees, agents, affiliates, partners and managers for any third-party claims arising out of your usage of the WHOIS privacy services.

d. PARKED DOMAINS: We offer a service to park your domains. In choosing to park your domains with us, we will create and host a mini-site that will be displayed any time there is a visitor to your domain. Any domains that you park with us will automatically have their nameservers adjusted to our default settings, so please make sure you understand that any then-existing services for your domains prior to the nameserver change will stop functioning.
Ads will be displayed on your parked mini-sites. You will have the opportunity to have ads inserted from your advertising account which will allow you to keep 100% of that advertising revenue. If you fail to configure one or more of the available ad slots, we will have the option of serving our own ads which will entitle us to all of those advertising proceeds.

You will also be able to configure your parked pages to include your own content as well as content that we make available. Parking your domains with us implies your acceptance of the following points:

a. You will not add any profanity, copyrighted content, or anything else, which in our sole discretion, is harmful, profane or illegal.

b. We reserve the right to remove or modify your parked domain status or any content on your parked mini-sites at any time and for any reason. Although not obligated to do so, in such an event we will make a reasonable effort to contact you to let you know about our decision and to either give you time to change the offending content, or to make other plans for the use of your domain name.

e. DOMAIN DEFENDER: We offer a service called Domain Defender which you can optionally enable for your account. This service allows you to add extra security to your account by selecting supplemental security questions and associated answers that must be answered before making changes through your account. Additionally, you can configure the service to optionally send you e-mail and/or text messages upon the completion of certain changes to your domains. Your use of this service is entirely optional, but, if you choose to enable the service, the following applies:

a. We make NO CLAIM that use of the service will prevent misuse of your account or unintended changes to your domains. Your responsibilities within this Agreement to secure your account are still in force.

b. If you select to receive text message notifications, you understand that all messaging rates imposed by your carrier will apply.

c. We are not responsible for any notifications that you do not receive, including but not limited to, emails that are caught in an anti-spam system and text messages not delivered by your carrier.

d. Even with this service enabled, we still highly recommend locking all of your domains.

5. SERVICES PROVIDED AT WILL; TERMINATION OR SUSPENSION OF SERVICES:

a. We may reject your domain name registration application or elect to discontinue providing Services to you for any reason within 30 days of a Service initiation or a Service renewal. Outside of this period, we may terminate or suspend the Services at any time for cause, which, without limitation, includes (i) registration of prohibited domain name(s), (ii) abuse of the Services, (iii) payment irregularities, (iv) illegal conduct, (v) failure to keep your Account or WHOIS information accurate and up to date, (vi) failure to respond to inquiries from us for over three (3) calendar days, (vii) if your use of the Services involves us in a violation of any third party's rights or acceptable use policies, including but not limited to the transmission of unsolicited email, the violation of any copyright, or the distribution of any form of malware (defined to include, without limitation, malicious code or software that

Feedback On the New Site?
This site uses cookies to provide you with a better user experience. For more information, refer to our Privacy Policy
Confirm

liability, civil or criminal, on the part of us, as, well as its affiliates, subsidiaries, officers, directors, and employees, (x) to protect the integrity, security and stability of the Domain

Name system (DNS), or (xi) failure to respond to inquiries from us regarding payment inquiries for over 24 hours.
Prohibited domain names and illegal activities which may be subject to these provisions include, but are not limited to:

i. Domains and web sites prohibited by the laws of the United States and/or foreign territories in which you conduct business
ii. Domains and web sites designed to encourage unlawful behavior by others, such as hate crimes, terrorism and child pornography
iii. Domains and web sites that are tortious or invasive of the privacy of a third party
iv. Domains and web sites designed to harm or use unethically minors in any way
v. Domains and web sites involved in the transmission of unsolicited email
vi. Domains and web sites involved in unauthorized repetitive, high volume inquires into any of the services provided by us or a third-party
vii. Domains and web sites involved in copyright and/or trademark infringement
viii. Domains transferred illegally from a different registrar without the previous Registrant's knowledge

REFUNDS WILL NOT BE ISSUED IF YOUR SERVICES ARE SUSPENDED FOR CAUSE PER THIS AGREEMENT.

THERE ARE ABSOLUTELY NO REFUNDS FOR BITCOIN PURCHASES.

If we determine that your account is engaged in repeated abuse of this Agreement then we may elect to terminate your entire account and all domains within your account.

b. You may cancel any domain registration (other than domains registered via drop-catching) with us within three (3) days of purchase for a full refund (minus any applicable transaction fees). You may cancel at any time after the three-day period, but no refund will be issued. To cancel a domain name, please log in to your account and visit the Order History page. Your refund will be issued back to the method of payment used to make the registration purchase. The total refund amount may be reduced by any transaction fees that we incurred as part of the initial transaction and/or the issuance of the refund. All refunds will go back to the source of the transaction.

Important note regarding domain registration refunds. At our sole discretion, we may choose not to issue a domain registration refund if we believe you to be engaged in "domain tasting" or some other activity resulting in an abnormal number of cancellations. More specifically, if, in our sole discretion, we believe you to be engaged in a high volume or irregular number of registrations and subsequent cancellations, we may opt not to refund your money. In the event we believe you to be engaged in such activity, we will make an effort to issue one warning via email to you prior to disallowing further refunds for your account, but we are not obligated to do so.

c. You may cancel domain renewals (other than renewals associated with Expired Domain Auctions) with us within three (3) days of purchase for a full refund (minus any applicable transaction fees). If you transfer your domain within 45 days of a domain renewal, you may not be entitled to a refund and you may also not receive any extended registration time on your domain. ALL DOMAIN RENEWAL CANCELLATIONS, OTHER THAN CERTAIN AUTOMATIC RENEWALS, WILL RESULT IN YOUR DOMAIN BEING DELETED AND PLACED INTO THE REDEMPTION PERIOD AT THE REGISTRY. THIS MEANS THAT YOU WILL NOT BE ABLE TO RENEW THE DOMAIN WITH US WITHOUT PAYING FOR A RESTORATION, OR POSSIBLY NOT AT ALL. IF YOU HAVE TIME REMAINING ON YOUR REGISTRATION IT WILL BE SACRIFICED IN TOTAL WHEN RECEIVING A RENEWAL REFUND.

Important note regarding domain renewal refunds. At our sole discretion, we may choose not to issue a domain renewal refund if your cancellation rate surpasses the ratios set by our system.

d. Sorry, but refunds are not available for restorations, completed transfers, Sedo premium domains, Afternic premium domains, domain auctions and marketplace purchases or Bitcoin purchases.

e. If we terminate or suspend the Services provided to you under this Agreement, we may then, at our option, make either ourselves or a third party the beneficiary of Services which are substantially similar to those which were previously provided to you. If we have grounds to terminate or suspend Services with respect to one domain name or in relation to other Services provided through your Account, we may terminate or suspend all Services provided through your Account. No fee refund will be made when there is a suspension or termination of Services for cause.

f. At any time and for any reason, we may terminate the Services thirty (30) days after we send notice of termination via mail or email, at our option, to the WHOIS contact information provided in association with your domain name registration. Following notice of termination other than for cause, you must transfer your domain name within such thirty (30) day notice period or risk that we may delete your domain name, transfer the registration services associated with your domain name to ourselves or a third party, or suspend or modify Services related to your domain name. If we terminate Services for a

Feedback On the New Site?
This site uses cookies to provide you with a better user experience. For more information, refer to our Privacy Policy
Confirm

registrar or registry administrator procedures approved by an ICANN-adopted policy or any policy adopted by any ccTLD registry or governing body, to correct mistakes by us, another

registrar or the registry administrator in administering the domain name or for the resolution of disputes concerning the domain name or as a result of any government decree, rule, law or regulation. This includes, but is not limited to, ICANN's WHOIS ACCURACY PROGRAM SPECIFICATION which requires that we deactivate any domains for which we have not received verification of Registrant email address within 15 days of notification.

6. FEES: You agree to pay, prior to the effectiveness of the desired Services, the applicable Service fees set forth during the registration process or otherwise communicated to you by us. In the event any of the fees for Services change, we will use reasonable efforts to give you thirty (30) days prior notice of such a change. All fees are non-refundable, in whole or in part, even if your domain name registration is suspended, cancelled or transferred prior to the end of your then current registration term, unless this Agreement specifically provides for a refund. At our option, we may require that you pay fees through a particular payment means (such as by credit card or by wire transfer) or that you change from one payment provider to another.

   PREMIUM DOMAINS: Please note that it is possible that the pricing shown on our web site's pricing or search results pages may not be the actual price for a registation, transfer or renewal. This happens when the registry for a domain determines that a specific domain is a "premium domain". If this happens, our system will notify you and update the pricing in your shopping cart as soon as the domain is added. We recommend always checking the price in the shopping cart when adding to or changing your order.
7. PAYMENT ISSUES: In the event of a charge back, or if we have belief in an imminent charge back, by a credit card company, credit card holder, or similar action by another payment provider, including, but not limited to PayPal, Payza or Skrill investigations, allowed by us in connection with your payment of fees for any Services, we may suspend access to any and all Accounts you have with us and all interests in and use of any domain name registration services. We may cancel any order(s) associated with anything covered in this section, but may not provide a refund. We may reinstate your rights to and control over these Services solely at our discretion, and potentially subject to our receipt of the unpaid fees and our then-current reinstatement fee as otherwise communicated to you by us. If you have an issue with credit card or other payment charges, you should contact us regarding the issue before you contact your credit card or other payment process company to request a charge back or reversal of the charges.
8. EXPIRATION AND RENEWAL OF SERVICES: It is your responsibility to keep your own records and to maintain your own reminders regarding when your domain name registration or other Services are set to expire and to maintain current and accurate credit card information should any Services be placed on "auto-renew." As a convenience to you, and not as a binding commitment, we may notify you via an email message or via your Account when renewal fees are due. Should these fees go unpaid, your Services will expire or be cancelled. Payment must be made by credit card, account funds, Paypal, or such other method as we may allow or require from time to time. If you select automatic renewal of the Services, we may attempt to renew the Services a reasonable time before expiration, provided your billing information is available and up to date. It is your responsibility to keep your billing information up to date and we are not required to, but may, contact you to update this information in the event that an attempted transaction is not processed successfully.
9. EXPIRATION OF A DOMAIN NAME REGISTRATION: Immediately after the expiration of the term of domain name registration services and before deletion of the domain name in the applicable registry's database, we may stop publishing zone files for your domain, direct the domain name to name-servers and IP address(es) designated by us, including, without limitation, to no IP address or to IP address(es) which host a parking page or a commercial search engine that may display advertisements, and we may either leave your WHOIS information intact or we may change the contact information in the WHOIS output for the expired domain name so that you are no longer the listed registrant of the expired domain name.

   a. Reactivation Period Process. For a period of approximately 30 days after expiration of the term of domain name registration services, we may provide a procedure by which expired domain name registration services may be renewed. We may, but are not obligated to, offer this process, called the "reactivation period." You assume all risks and all consequences if you wait until close to or after the expiration of the original term of domain name registration services to attempt to renew the domain name registration services. We may, in our sole discretion, choose not to offer a reactivation period and we shall not be liable therefore. The reactivation period renewal process, if any, may involve additional fees which we will solely determine. We may make expired domain name services(s) available to third parties, we may auction off the rights to expired domain name services, and/or expired domain name registration services may be re-registered to any party at any time.
      - You can find our renewal pricing on our pricing page
      - You can find our restoration/redemption pricing and our schedule to deliver pre- and pos-expiraiton notifications on our expiration process page
   b. If you select to deactivate your domain name, we reserve the right to place any such deactivated domain names into our expired domain marketplace upon expiraiton. As with all expired domain marketplace sales, you will not receive any compensation if the domain sells.

Feedback On the New Site?
This site uses cookies to provide you with a better user experience. For more information, refer to our Privacy Policy
Confirm

discontinued domain name registration services may nonetheless be renewed. We may, but are not obligated to, participate in this process, typically called the "Redemption Grace Period" ("RGP"). We may, in our sole discretion, choose not to participate in the RGP process with respect to any or all of your domain name registration services and we shall not be liable therefore. If available, RGP typically ends between 30 and 42 days after the end of the reactivation period of the domain name services. We are not obliged to contact you to alert you that the domain name registration services are being discontinued; or

ii. Pay the registry's registration fee or otherwise provide for the registration services to be continued. In which case, we may then set the name-servers and the DNS settings for the domain name services, we may set the DNS to point to no IP address or to IP address(es) which host parking page(s) or a commercial search engine that may display paid advertisements, and we may change the contact information in the WHOIS output for the expired domain name so that you are no longer the listed registrant of the expired domain name. We do not have to pay you any of the proceeds we may earn as a result. We are not obliged to contact you to alert you that the domain name registration services are being continued. The domain name will be designated as being in the extended redemption grace period ("ERGP"), and you will be allowed to assume, during the first 120 days of the then extant registration term, complete management of the domain name services, including the right to control the DNS settings, provided that you pay the fees we set forth plus any registration fees. After the end of the 120-day period, if you do not exercise your rights under this provision, you have abandoned the domain name services, and relinquish all interests and use of the domain name services; or

iii. Auction the domain name to a third party which entails transferring the domain name registration services to such third party. In which case, the third party who won the auction for the domain name services will become the new Registrant of the domain name, and you will lose any claim to that domain. In the event we auction your domain and assign it to a third-party, we may, but are not required to, inform you that such a transition has occurred. You can find our domain expiration process listed on our web site, and it remains your responsibility to renew your domain names on time to avoid losing them.

10. TRANSFERS:

a. Transfer of your domain name(s) services shall be governed by ICANN's transfer policy, available at http://www.icann.org/transfers/, including the Registrar Transfer Dispute Resolution Policy, available at https://www.icann.org/resources/pages/transfer-policy-2016-06-01-en as well as the UDRP as described in the Dispute Resolution Policy of this Agreement, as these policies may be modified from time to time. To transfer your domain name(s) you should first login to your Account to lock or unlock your domain name(s) and/or to obtain the EPP "AuthCode" which is required to transfer domain services in an EPP registry (such as .org). Only the registrant and the administrative contacts listed in the WHOIS information may approve or deny a transfer request. Without limitation, domain name services may not be transferred within 60 days of initial registration, within 60 days of a transfer, if there is a dispute regarding the identity of the domain name registrant, if you are bankrupt, or if you fail to pay fees when due. We will follow the procedures for both gaining and losing registrars as outlined in ICANN's transfer policies. A transfer will not be processed if, during this time, the domain name registration services expire, in which event you may need to reinstate the transfer request following a redemption of the domain name, if any. You may be required to resubmit a transfer request if there is a communication failure or other problem at either our end or at the registry. YOU ASSUME ALL RISK FOR FAILURE OF A TRANSFER WHETHER OR NOT THE TRANSFER PROCESS IS INITIATED CLOSE TO THE END OF A REGISTRATION TERM.

b. We may place a "Registrar Lock" on your domain name services and this will prevent your domain name services from being transferred without your authorization, though we are not required to do so. By allowing your domain name services to remain locked, you provide express objection to any and all transfer requests until the lock is removed.

c. You may cancel incoming transfer requests at any time before they are completed up to 59 calendar days from the initial transfer order. Canceling a transfer request will entitle you to a refund of the transfer cost, minus processing fees. YOU WILL NOT BE ENTITLED TO A REFUND IF YOU CANCEL YOUR TRANSFER REQUEST AFTER THE 59 DAY TIME LIMIT.

d. In the event we receive a request from a different registrar to transfer your domain away, you may be presented with an option to approve the transfer without waiting the standard 5-7 days for registry release. Any such approval grants us the right to approve the transfer immediately. We also reserve the right to approve outbound transfers at any time during the transfer process. In the event either you or we approve an outbound transfer, the transfer will complete within 15 minutes.

e. Certain transfers may not be eligible for the 1-year extension associated with most transfers. For example, domains renewed within 45 days of transfer or domains already registered for more than 9 years will not get extended by a year upon transfer completion. Registries apply the extra year, registrars do not. Therefore, if the registry is unable to extend the expiration by a year, then one year will not be added to your domain transfer.

11. DNS SERVICES: The Domain Name System (DNS) is a hierarchical naming system built on a distributed database for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most importantly, it translates domain names meaningful to humans into the numerical identifiers associated with networking equipment for the purpose of

Feedback On the New Site?
This site uses cookies to provide you with a better user experience. For more information, refer to our Privacy Policy
Confirm

provider at any time by associating different authoritative name servers with the applicable domains as needed. By using the DNS service we offer, you hereby acknowledge and agree to the following:

a. DNS is a critical service responsible for all facets of domain use. Incorrect configuration of DNS as it relates to your domains can lead to problems such as:
   i. Web site(s) not loading
   ii. Email can stop working
b. You should only make DNS modifications if you fully understand the implications of doing so, understand how DNS works, have the technical expertise to verify the modifications were propagated properly to the associated authoritative name servers, and are prepared to fully test the impact of the modifications as soon as they take effect.
c. We make absolutely no guarantee whatsoever related to the DNS hosting service. If you need a service level agreement guaranteeing minimum performance or reliability levels, you should use a different DNS service provider who offers such guarantees.
d. DNS is a globally distributed database with many interconnected components - the vast majority of which are NOT directly or indirectly under our control. Problems can occur anywhere in the system.
e. Many of the distributed nodes in DNS, commonly referred to as recursive resolvers, cache DNS resource records for the time recommended by our authoritative name servers (controlled via the TTL value), or for any amount of time they are configured to do so (they can ignore our recommended time). As a result, changes made to DNS records through us will not immediately propagate to your local systems - the delay can be as long as the maximum TTL setting on the associated records, or longer.
f. We, at our sole discretion, reserve the right to provide additional support for DNS related matters, or no support at all.
g. Upon domain deletion, domain expiration, transfer of a domain (away from us), and/or the cancellation/termination/suspension/deletion of your account(s), DNS service for the associated domain(s) and/or account(s) will be terminated. It is entirely your responsibility to make alternative DNS service arrangements prior and/or after termination of DNS service as needed if said termination could affect you in any way.
h. We, at our sole discretion, reserve the right to make any changes to DNS records we deem necessary to protect the stability of our system.

DNS Service Disclaimer of Warranty

THERE IS NO WARRANTY FOR THE DNS SERVICE, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING WE PROVIDE THE DNS SERVICE "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE DNS SERVICE IS WITH YOU. SHOULD THE DNS SERVICE PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

DNS Service Indemnification

We use the systems of a third party, DNSOwl.com, to provide all DNS services. You agree to indemnify, defend and hold harmless DNSOwl.com, and its directors, officers, employees, agents, and affiliates from and against any and all claims, damages, liabilities, costs and expenses, including reasonable legal fees and expenses arising out of or relating to your domains and/or any DNS related matter.

12. OWNERSHIP OF INFORMATION AND DATA: We own all database, compilation, collective and similar rights, title and interests worldwide in our domain name database, and all information and derivative works generated from the domain name database. We own the following information for those registrations for which we are the registrar: (a) the original creation date of the registration, (b) the expiration date of the registration, (c) the name, postal address, e-mail address, voice telephone number, and where available fax number of the registrant and all contacts for the domain name registration, (d) any remarks concerning the registered domain name that appear or should appear in the WHOIS or similar database, and (e) any other information we generate or obtain in connection with the provision of Services, other than the domain name being registered, the IP addresses of the primary nameserver and any secondary nameservers for the domain name, and the corresponding names of those nameservers. We do not have any ownership interest in your specific personal registration information outside of our rights in our domain name database.
13. AGENTS AND LICENSES: If you are registering a domain name for or on behalf of someone else, you represent that you have the authority to bind that person as a principal to all terms and conditions provided herein. If you license the use of a domain name you register to us or a to third party, you remain the domain name holder of record, and remain responsible for all obligations at law and under this Agreement, including but not limited to payment obligations, and providing (and updating, as necessary) both your own full contact information, and accurate technical, administrative, billing and zone contact information adequate to facilitate timely resolution of any problems that arise in connection with the domain name and domain name registration and for ensuring non-infringement of any third

Feedback On the New Site?
This site uses cookies to provide you with a better user experience. For more information, refer to our Privacy Policy
Confirm

providing the Registered Name Holder reasonable evidence of actionable harm.

You authorize us to serve as your "Designated Agent" permitting us to approve any "Change of Registrant". The terms "Designated Agent" and "Change of Registrant" used in this Section are defined in the ICANN transfer policy seen here . Due to your authorization for us to serve as your "Designated Agent", Registrants will not need to receive an email concerning the change, and will also not need to confirm the change via email. We will instead auto-approve any "Changes of Registrant". You further explicity opt-out of an inter-registrar transfer lock as would otherwise have been required per the ICANN transfer policy linked to above.

14. LIMITATION OF LIABILITY: WE WILL NOT BE LIABLE FOR ANY (a) SUSPENSION OR LOSS OF THE SERVICES, (b) USE OF THE SERVICES, (c) INTERRUPTION OF SERVICES OR INTERRUPTION OF YOUR BUSINESS, (d) ACCESS DELAYS OR ACCESS INTERRUPTIONS TO OUR WEB SITE(S) OR SERVICES OR DELAYS OR ACCESS INTERRUPTIONS YOU EXPERIENCE IN RELATION TO A DOMAIN NAME REGISTERED WITH US; (e) LOSS OR LIABILITY RESULTING FROM ACTS OF OR EVENTS BEYOND OUR CONTROL (f) DATA NON-DELIVERY, MIS-DELIVERY, CORRUPTION, DESTRUCTION OR OTHER MODIFICATION; (g) THE PROCESSING OF AN APPLICATION FOR A DOMAIN NAME REGISTRATION; (h) LOSS OR LIABILITY RESULTING FROM THE UNAUTHORIZED USE OR MISUSE OF YOUR ACCOUNT IDENTIFIER OR PASSWORD; OR (i) APPLICATION OF ANY DISPUTE POLICY. WE WILL NOT BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND (INCLUDING LOST PROFITS) REGARDLESS OF THE FORM OF ACTION WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL OUR MAXIMUM AGGREGATE LIABILITY EXCEED THE TOTAL AMOUNT PAID BY YOU FOR SERVICES, AND IN NO EVENT SHALL OUR LIABILITY BE GREATER THAN $200.00 (US Dollars). BECAUSE SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, IN SUCH STATES, OUR LIABILITY SHALL BE LIMITED TO THE MAXIMUM EXTENT PERMITTED BY LAW.
15. INDEMNITY: You hereby release, indemnify, and hold us, ICANN, the registry operators (including, but not limited to VeriSign, Inc), as well as the contractors, agents, employees, officers, directors, shareholders, and affiliates of such parties harmless from and against any and all liabilities, claims, damages, costs and expenses, including reasonable attorneys' fees and court costs, for third party claims relating to or arising under this Agreement, including any breach of any of your representations, warranties, covenants or obligations set forth in this Agreement, the Services provided hereunder (including, but not limited to WHOIS privacy), or your use of the Services, including, without limitation, infringement by you, or by anyone else using the Services, of any intellectual property or other proprietary right of any person or entity, or from the violation of any of our or ICANN's operating rules or policies relating to the Services provided. We may seek written assurances from you in which you promise to indemnify and hold us harmless from the costs and liabilities described in this paragraph. Such written assurances may include, in our sole discretion, the posting of a performance bond(s) or other guarantees reasonably calculated to guarantee payment. Your failure to provide such assurances may be considered by us to be a breach of this Agreement by you and may, in our sole discretion, result in loss of your right to control the disposition of domain name Services for which you are the registrant and in relation to which we are the registrar of record. This indemnification is in addition to any indemnification (a) required under the UDRP or any other ICANN policy or any policy of any relevant registry; or (b) set forth elsewhere in this Agreement.
16. REPRESENTATIONS AND WARRANTIES: YOU REPRESENT AND WARRANT THAT NEITHER THE REGISTRATION OF A DOMAIN NAME NOR THE MANNER IN WHICH IT IS DIRECTLY OR INDIRECTLY USED NOR THE USE OF OTHER OF THE SERVICES INFRINGES THE LEGAL RIGHTS OF A THIRD PARTY OR WILL OTHERWISE SUBJECT US TO A LEGAL CLAIM. THE SERVICES ARE INTENDED FOR USE BY PERSONS WHO ARE AT LEAST 18 YEARS OLD AND BY USING THE SERVICES, YOU REPRESENT AND WARRANT THAT YOU ARE AT LEAST 18 YEARS OLD AND ALL INFORMATION PROVIDED BY YOU IN CONNECTION WITH YOUR PROCUREMENT OF THE SERVICES IS ACCURATE. ALL SERVICES ARE PROVIDED TO YOU "AS IS" AND WITH ALL FAULTS. EXCEPT FOR OUR STATEMENT REGARDING OUR ACCREDITATION AS ICANN-APPROVED DOMAIN NAME REGISTRARS, WE MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHATSOEVER, EXPRESS OR IMPLIED, IN CONNECTION WITH THIS AGREEMENT OR THE SERVICES, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, UNLESS SUCH REPRESENTATIONS AND WARRANTIES ARE NOT LEGALLY EXCLUDABLE. WITHOUT ANY LIMITATION TO THE FOREGOING, WE MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHATSOEVER THAT REGISTRATION OR USE OF A DOMAIN NAME UNDER THIS AGREEMENT WILL IMMUNIZE YOU EITHER FROM CHALLENGES TO YOUR DOMAIN NAME REGISTRATION, OR FROM SUSPENSION, CANCELLATION OR TRANSFER OF THE DOMAIN NAME REGISTERED TO YOU. ANY MATERIAL AND/OR DATA DOWNLOADED OR OTHERWISE OBTAINED THROUGH THE USE OF OUR E-MAIL FORWARDING OR OTHER EMAIL SERVICE IS DONE AT YOUR OWN DISCRETION AND RISK AND YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO YOUR COMPUTER SYSTEM OR LOSS OF DATA THAT RESULTS FROM THE DOWNLOAD OF SUCH MATERIAL AND/OR DATA. WE MAKE NO WARRANTY REGARDING ANY GOODS OR SERVICES PURCHASED OR OBTAINED THROUGH OUR E-MAIL SERVICES OR ANY TRANSACTIONS ENTERED INTO THROUGH OUR E-MAIL SERVICES. NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED BY YOU FROM US SHALL CREATE ANY WARRANTY NOT

Feedback On the New Site?
This site uses cookies to provide you with a better user experience. For more information, refer to our Privacy Policy
Confirm

policies of any relevant registry, including but not limited to the Uniform Domain Name Dispute Resolution Policy ("UDRP"), which is available at http://www.icann.org/udrp/udrp-rules-24oct99.htm and http://www.icann.org/dndr/udrp/policy.htm along with the UDRP Rules and all Supplemental Rules of any UDRP provider. The UDRP may be changed by ICANN (or ICANN's successor) at any time. If the registration or reservation of your domain name is challenged by a third party, you will be subject to the provisions specified in the UDRP in effect at the time your domain name registration is disputed by the third party. In the event a domain name dispute arises with any third party, you will indemnify and hold us harmless pursuant to the terms and conditions of the UDRP. If you or your domain name are the subject of litigation, we may deposit control of your domain name record into the registry of the judicial body by providing a party with a registrar certificate.

18. GOVERNING LAW AND JURISDICTION FOR DISPUTES:

    a. Except as otherwise set forth in the UDRP or any similar ccTLD policy, with respect to any dispute over a domain name registration, this Agreement, your rights and obligations and all actions contemplated by this Agreement shall be governed by the laws of the United States of America and the State of Arizona, as if the Agreement was a contract wholly entered into and wholly performed within the State of Arizona.

    b. Any dispute, claim or controversy arising out of or relating to this Agreement or the breach, termination, enforcement, interpretation or validity thereof, including the determination of the scope or applicability of the agreement to arbitrate, shall be determined by arbitration in Maricopa County, Arizona, before one arbitrator. The arbitration shall be administered by JAMS pursuant to its Comprehensive Arbitration Rules and Procedures. Judgment on the Award may be entered in any court having jurisdiction. This clause shall not preclude us from seeking provisional remedies in aid of arbitration from a court of appropriate jurisdiction. Service of process on you by us in relation to any dispute arising under this Agreement may be served upon you by first class mail to the address listed by you in your Account and/or domain name WHOIS information or by electronically transmitting a true copy of the papers to the email address listed by you in your Account and/or domain name WHOIS information.

    c. Notwithstanding the foregoing, for the adjudication of third party disputes (i.e., disputes between you and another party, not us) concerning or arising from use of domain names registered hereunder, you shall submit without objection, without prejudice to other potentially applicable jurisdictions, to the subject matter and personal jurisdiction of the courts (i) of the domicile of the registrant as it appears in the public WHOIS record for the domain name(s) in controversy, and (ii) where we are located.

    d. When contacting us, please refer to our abuse reporting procedures as listed on our web site if you are contacting us concerning abuse of our services. As such, and for any and all other legal notifications to our company, please use email or the form on our contact us page to contact us. Postal mail correspondence should be expected to incur delays.

19. NOTICES: Any notices required to be given under this Agreement by us to you will be deemed to have been given if sent in accordance with the Account and/or domain name WHOIS information you have provided.
20. PRIVACY: Details about how we process and share your information, options available to you regarding its use, as well as how to contact us, can be found in our privacy policy. By accepting this Agreement, you also accept the use of your information as described in our privacy policy. Furthermore, you hereby agree not to submit anybody else's personal information to us in conjunction with your use of Services without first communicating your intended use of their personal information along with our privacy policy and then obtaining their consent to said use.
21. GENERAL: This Agreement and all applicable ICANN policies and the policies of any relevant registry, including but not limited to the UDRP, together with all modifications, constitute the complete and exclusive agreement between you and us, and supersede and govern all prior proposals, agreements, or other communications. Nothing contained in this Agreement shall be construed as creating any agency, partnership, or other form of joint enterprise between the parties. The failure of us to require your performance of any provision hereof shall not affect the full right to require such performance at any time thereafter; nor shall the waiver by us of a breach of any provision hereof be taken or held to be a waiver of the provision itself. In the event that any provision of this Agreement shall be unenforceable or invalid under any applicable law or be so held by applicable court decision, such unenforceability or invalidity shall not render this Agreement unenforceable or invalid as a whole. We will amend or replace such provision with one that is valid and enforceable and which achieves, to the extent possible, our original objectives and intent as reflected in the original provision. This Agreement may not be amended or modified by you except by means of a written document signed by both you and an authorized representative of us.
22. DATES/TIMES: All dates/times shown in our sytem for information including, but not limited to, expiration dates, auction end times and transfer completion dates are based upon Arizona time unless otherwise noted.

Terms and conditions specific to .BIZ domain registrations

Registrations in the .BIZ TLD must be used or intended to be used primarily for bona fide business or commercial purposes. For purposes of the .BIZ Registration Restrictions ("Restrictions"), "bona fide business or commercial use" shall mean the bona fide use or bona fide intent to use the domain name or any content, software, materials, graphics or other information thereon, to permit Internet users to access one (1) or more host computers through the DNS:

Feedback On the New Site?
This site uses cookies to provide you with a better user experience. For more information, refer to our Privacy Policy
Confirm

iii. To facilitate (i) the exchange of goods, services, information, or property of any kind, or, (ii) the ordinary course of trade or business. Registering a domain name solely for the purposes of (1) selling, trading or leasing the domain name for compensation, or (2) the unsolicited offering to sell, trade or lease the domain name for compensation shall not constitute a "bona fide business or commercial use" of that domain name.

As a .BIZ domain name registrant, You hereby certify to the best of Your knowledge that:

i. The registered domain name will be used primarily for bona fide business or commercial purposes and not (i) exclusively for personal use; or (ii) solely for the purposes of (1) selling, trading or leasing the domain name for compensation, or (2) the unsolicited offering to sell, trade or lease the domain name for compensation. More information on the .BIZ restrictions, which are incorporated herein by reference, are available online.
ii. The domain name registrant has the authority to enter into the registration agreement; and
iii. The registered domain name is reasonably related to the registrant's business or intended commercial purpose at the time of registration.

Domain Name Dispute Policy

If You reserved or registered a .BIZ domain name through us, You agree to be bound by our current domain name dispute policy that is incorporated herein and made a part of this Agreement by reference. Please take the time to familiarize Yourself with that policy. In addition, You hereby acknowledge that You have read and understood and agree to be bound by the terms and conditions of the following documents, as they may be amended from time to time, which are hereby incorporated and made an integral part of this Agreement:

i. The Uniform Domain Name Dispute Policy;
ii. The Start-up Trademark Opposition Policy ("STOP"); and
iii. The Restrictions Dispute Resolution Criteria and Rules.

The STOP sets forth the terms and conditions in connection with a dispute between a registrant of a .BIZ domain name ("Registrant") with any third party (other than Registry Operator or Registrar) over the registration or use of a .BIZ domain name registered by Registrant that is subject to the Intellectual Property Claim Service. The Intellectual Property Claim Service is a service introduced by Registry Operator to notify a trademark or service mark holder ("Claimant") that a second-level domain name has been registered in which that Claimant claims intellectual property rights. In accordance with the STOP and its associated Rules, those Claimants will have the right to challenge registrations through independent ICANN-accredited dispute resolution providers.
The UDRP sets forth the terms and conditions in connection with a dispute between a Registrant and any party other than the Registry Operator or Registrar over the registration and use of an Internet domain name registered by Registrant.

The RDRP sets forth the terms under which any allegation that a domain name is not used primarily for business or commercial purposes shall be enforced on a case-by-case, fact specific basis by an independent ICANN-accredited dispute provider. None of the violations of the Restrictions will be enforced directly by or through Registry Operator. Registry Operator will not review, monitor, or otherwise verify that any particular domain name is being used primarily for business or commercial purposes or that a domain name is being used in compliance with the SUDRP or UDRP processes.**Domain Name Dispute Policy Modifications**

You agree that we, in our sole discretion, may modify our dispute policy. We will post any such revised policy on our web site at least thirty (30) calendar days before it becomes effective. You agree that, by maintaining the reservation or registration of Your domain name after modifications to the dispute policy become effective, You have agreed to these modifications. You acknowledge that if You do not agree to any such modification, You may terminate this Agreement. We will not refund any fees paid by You if You terminate Your Agreement with us.

Domain Name Disputes

You agree that, if Your use of our domain name registration services is challenged by a third party, You will be subject to the provisions specified in our dispute policy in effect at the time of the dispute. You agree that in the event a domain name dispute arises with any third party, You will indemnify and hold us harmless pursuant to the terms and conditions set forth below in this Agreement. If we are notified that a complaint has been filed with a judicial or administrative body regarding Your use of our domain name registration services, You agree not to make any changes to Your domain name record without our prior approval. We may not allow You to make changes to such domain name record until (i) we are directed to do so by the judicial or administrative body, or (ii) we receive notification by You and the other party contesting Your registration and use of our domain name registration services that the dispute has been settled. Furthermore, You agree that if You are subject to litigation regarding Your registration and use of our domain name registration services, we may deposit control of Your domain name record into the registry of the judicial body by supplying a party with a registrar certificate from us.

Reservation of Rights

We and the .BIZ Registry Operator, NeuLevel, Inc. expressly reserve the right to deny, cancel or transfer any registration that it deems necessary, in its discretion, to protect the integrity and stability of the registry, to comply with any applicable laws, government rules or requirements, requests of law enforcement, in compliance with any dispute resolution process, or to avoid any liability, civil or criminal, on the part of us and/or NeuLevel, Inc., as well as their affiliates

Feedback On the New Site?
This site uses cookies to provide you with a better user experience. For more information, refer to our Privacy Policy
Confirm

Indemnification

You agree to indemnify, defend and hold harmless the .BIZ Registry Operator, NeuLevel, Inc., and its directors, officers, employees, agents, and affiliates from and against any and all claims, damages, liabilities, costs and expenses, including reasonable legal fees and expenses arising out of or relating to the Registered Name holder's domain name registration. This indemnification requirement shall survive the termination or expiration of the registration agreement.

Terms and conditions specific to .COM and .NET domain registrations

You agree to indemnify, defend and hold harmless the .COM .and NET Registry Operator, VeriSign, Inc., and its directors, officers, employees, agents, and affiliates from and against any and all claims, damages, liabilities, costs and expenses, including reasonable legal fees and expenses arising out of or relating to the Registered Name holder's domain name registration.

Terms and conditions specific to Afilias domain registrations

You agree to the Afilias policies as found at http://afilias.info/policies.

Terms and conditions specific to .INFO domain registrations

You agree to indemnify, defend and hold harmless the .INFO Registry Operator, Afilias Limited, and its subcontractors, shareholders, directors, officers, employees, agents, and affiliates from and against any and all claims, damages, liabilities, costs and expenses, including reasonable legal fees and expenses arising out of or relating to the Registered Name holder's domain name registration. This indemnification requirement shall survive the termination or expiration of this Agreement.

If You are registering a .INFO domain name You also agree to:

1. consent to the use, copying, distribution, publication, modification and other processing of Registered Name Holder's Personal Data by the .info Registry Operator and its designees and agents;
2. submit to proceedings commenced under ICANN's Uniform Domain Name Dispute Resolution Policy ("UDRP") and the Sunrise Dispute Resolution Policy ("SDRP");
3. immediately correct and update the registration information for the Registered Name during the registration term for the Registered Name; and
4. acknowledge that the Registry Operator will have no liability of any kind for any loss or liability resulting from the proceedings and processes relating to the Sunrise Period or the Land Rush Period, including, without limitation: (a) the ability or inability of a registrant to obtain a Registered Name during these periods, and (b) the results of any dispute over a Sunrise Registration.

Terms and conditions specific to .MOBI domain registrations

You acknowledge and agree that You shall comply with the requirements, standards, policies, procedures and practices set forth in the dotmobi Style Guide, found here. You consent to the monitoring of Your website for compliance with the Style Guide.

Further, You acknowledge and agree the Style Guide is subject to modification by the dotmobi registry, and You acknowledge and agree that You will comply with any such changes in the time allotted.

You agree to indemnify to the maximum extent permitted by law, defend and hold harmless Registry Operator, and its directors, officers, employees and agents from and against any and all claims, damages, liabilities, costs and expenses, including reasonable legal fees and expenses, arising out of or relating to Your domain name registration and or use, and this indemnification obligation survives the termination or expiration of this Agreement;

You agree to indemnify, defend and hold harmless Registry Services Provider, its subsidiaries and affiliates, and the directors, officers, employees and agents or each of them, from and against any and all claims, damages, liabilities, costs and expenses, including reasonable legal fees and expenses, arising out of or relating to Your domain name registration and or use, and this indemnification obligation survives the termination or expiration of this Agreement;

Acknowledge and agree that notwithstanding anything in this Agreement to the contrary, mTLD Top Level Domain Ltd. ("dotmobi"), the Registry Operator of the .MOBI TLD, is and shall be an intended third party beneficiary of this Agreement. As such, the parties to this Agreement acknowledge and agree that the third party beneficiary rights of dotmobi have vested and that dotmobi has relied on its third party beneficiary rights under this Agreement in agreeing to us being a registrar for the .MOBI top-level domain. Additionally, the third party beneficiary rights of dotmobi shall survive any termination or expiration of this Agreement.

You agree to comply with ICANN requirements, standards, policies, procedures, and practices for which dotmobi has responsibility in accordance with the Registry Agreement between ICANN and dotmobi or other arrangement with ICANN.

You consent to the use, copying, distribution, publication, modification and other processing of Your personal data by dotmobi and its designees and agents in a manner consistent with the

Feedback On the New Site?

This site uses cookies to provide you with a better user experience. For more information, refer to our Privacy Policy

Confirm

domain name(s) during the registration term for each registered name.

You further agree to comply with operational standards, policies, procedures, and practices for the Registry TLD established from time to time by Registry Operator in a non-arbitrary manner as Registry Policies, applicable to all registrars and/or Registered Name Holders, and consistent with the Registry Agreement shall be effective upon thirty (30) days notice by Registry Operator to Registrar;

You acknowledge and agree that dotmobi and Affilias Limited, acting in consent with dotmobi, reserves the right to deny, cancel or transfer any registration that it deems necessary, in its discretion (i) to protect the integrity and stability of the registry; (ii) to comply with all applicable laws, government rules or requirements, requests of law enforcement, in compliance with any dispute resolution process; (iii) to avoid any liability, civil or criminal, on the part of dotmobi as well as its affiliates, subsidiaries, officers, directors, representatives, employees, and stockholders; (iv) for violations of the terms and conditions herein; (v) or to correct mistakes made by dotmobi or any registrar in connection with a domain name registration, and dotmobi also reserves the right to freeze a domain name during resolution of a dispute.

You acknowledge and agree to be bound by the terms and conditions of the initial launch and general operations of the Registry TLD, including without limitation the Limited Industry Launch, the Sunrise Period, the Land Rush Period, the Sunrise Dispute Resolution Policy, the Premium Name Allocation Process, and the General Registration Period, and further to acknowledge that Registry Operator and the Registry Service Provider has no liability of any kind for any loss or liability resulting from the proceedings and processes relating to the Limited Industry Launch, the Sunrise Period, the Land Rush Period, the Sunrise Dispute Resolution Policy, the Premium Name Allocation Process, and the General Registration Period including, without limitation: (a) the ability or inability of a registrant to obtain a Registered Name during these periods, and (b) the results of any dispute made during the limited industry launch or over a Sunrise Registration.

You acknowledge and agree if the domain name being registered is a dotMobi Premium Name, and as such is listed at http://mtld.mobi/domain/premium, then use of the domain is also subject to the terms and conditions of the dotMobi Premium Name Agreement (formerly known as the dotMobi Auction Agreement) posted here, which is incorporated by reference herein.

You acknowledge and agree that upon termination or expiration of the dotMobi Premium Name Agreement in accordance with the terms thereof: (i) any and all rights of Company to the Registration of the Domain Name, the Registration Code, and/or to create, launch, and/or operate the web site shall be terminated, and all such rights shall revert to mTLD and (ii) mTLD may grant Registration rights to the Domain Name and/or rights to the Registration Code to any entity or person in its sole discretion, and Company shall have no rights or recourse against mTLD and/or Registrar relating to the registration or use of the Domain Name and/or Registration Code by any other such entity or person.

You Acknowledge and agree that Proxy or Proxy Registrations will not be allowed during the Sunrise Period, the Limited Industry Launch and the Premium Name Allocation and Auction Period, and in such an instance will constitute a material breach to this Agreement.

Terms and conditions specific to .ORG domain registrations

You agree to indemnify, defend and hold harmless the .ORG Registry Operator, Public Interest Registry, and its subcontractors, shareholders, directors, officers, employees, agents, and affiliates from and against any and all claims, damages, liabilities, costs and expenses, including reasonable legal fees and expenses arising out of or relating to the Registered Name holder's domain name registration. This indemnification requirement shall survive the termination or expiration of this Agreement.

Terms and conditions specific to .TICKETS domain registrations

WHOIS privacy is not permitted for .tickets registrations. There are further WHOIS verification steps that are required as noted at http://nic.tickets/pdfs/3.-Whois-Verification-and-Domain-Name-Allocation-Rules-During-General-Availability.pdf.

Terms and conditions specific to .US domain registrations

Indemnification. You agree to indemnify, defend, and hold harmless NeuStar, Inc., and its directors, officers, employees, representatives, agents, affiliates, and stockholders from and against any and all claims, suits, actions, other proceedings, damages, liabilities, costs and expenses of any kind, including without limitation reasonable legal fees and expenses, arising out of or relating to your (i) .us domain name registration, and (ii) use of any .us registered domain name.

.US Certification of U.S. Nexus. You certify that you have and shall continue to have a lawful bona fide U.S. Nexus in order to qualify to register and maintain use of a .us registered domain name. You must be, and you certify that you are, either:

1. (a) A natural person (i) who is a United States citizen, (ii) a permanent resident of the United States of American or any of its possessions or territories, or (iii) whose primary place of domicile is in the United States of America or any of its possessions ("Nexus Category 1"); or

About NameSilo
Account Options
Ordering / Shopping Cart
Domain Manager
Email
General Terms
Terms & Conditions
ICANN
WHOIS
WHOIS-Email-Verification
Premium nTLD Frequently Asked Questions
Policies

Feedback On the New Site?
This site uses cookies to provide you with a better user experience. For more information, refer to our Privacy Policy
Confirm

America, the District of Columbia, or any of its possessions or territories ("Nexus Category 2"); or,

3. (c) An entity or organization (including federal, state, or local government of the United States, or a political subivision thereof) that has a bona fide presence in the United States of America or any of its possessions or territories ("Nexus Category 3"). If you are claiming Nexus Category 3, you certify that you have a "bona fide presence in the United States" on the basis of real and substantial lawful contacts with, or lawful activities in, the United States of America, including, but not limited to, the sale of goods or services or other business, commercial or non-commercial including not-for-profit activities, or maintaining an office or other facility within the United States.

.US Certification of Name Servers Located in the U.S. you certify that the name servers listed by you for any .us domain name registration are located within the United States of America.

.US Certification of Accuracy of Registration Information. You acknowledge and agree that we have requested certain information from you during the .us domain name registration process in order to meet the above Nexus requirement, and that you have willingly volunteered such information. You acknowledge and agree that such information will be verified for accuracy and for compliance with the Nexus requirement and will be shared with NeuStar, Inc. You acknowledge and agree that, in order to implement the above Nexus requirement, NeuStar, Inc., will conduct "spot checks" on registrant information.

You understand and agree that your willful or grossly negligent provision of inaccurate or unreliable information, or your willful or grossly negligent failure to promptly update information, provided to us shall constitute a material breach of this Agreement and shall be a basis for cancellation of the domain name registration, without refund or credit to you. You further understand and agree that if such information cannot be verified for any reason, or if you fail to continue to abide by the Nexus requirements, the domain name registration may be subject to immediate "hold", rejection, or deletion by either us or NeuStar, Inc., without refund or credit to you. Neither we nor NeuStar, Inc., shall be liable to you for any actions or inactions resulting from your failure to satisfy all Nexus requirements or to provide all required Nexus requirement information in connection with the domain name registration. Neither we nor NeuStar, Inc., shall have any obligation to you to request or attempt to obtain from you additional information in order to establish your compliance with the Nexus requirements.

.US Dispute Policy. You agree to be bound by the Nexus Dispute Policy ("NDP") (located at http://www.neustar.us/policies/index.html), which will be administered solely by NeuStar, Inc., or its designated representative.

.US Restrictions. You acknowledge and agree that you are not permitted to purchase or use Domain Privacy service in connection with any .us domain name registration.

.US Reservation of Rights. NeuStar, Inc., reserves the right to "hold", deny, cancel, or transfer any registration that it deems necessary, in its sole discretion. You acknowledge and agree that we shall not be liable to you or any other party in connection with claims, damages, losses, expenses or costs incurred or suffered by you as a result of actions taken or not taken by NeuStar, Inc., or other third parties.

Terms and conditions specific to Rightside Registry domain registrations

Click here to review the Rightside Registry Terms and Conditions.

Terms and conditions specific to Donuts Inc. TLD domain registrations

Indemnification. You agree to indemnify (within 30 days of demand), defend, and hold harmless Donuts Inc., Donuts' service providers, Registrar and their respective affiliates and subsidiaries, as well as each of their respective owners, directors, managers, officers, employees, contractors, service providers and agents from and against any and all claims, damages, liabilities, costs and expenses, including reasonable legal fees and expenses (including on appeal), arising out of or relating in any way to the Registrant's domain name registration, including, without limitation, the use, registration, extension, renewal, deletion, and/or transfer thereof and/or the violation of any applicable terms or conditions governing the registration.

You will direct any disputes relating to the use of domain names to ICANN's Uniform Rapid Suspension System (http://newgtlds.icann.org/en/applicants/urs) or Uniform Domain Name Dispute Resolution Policy (http://www.icann.org/en/help/dndr/udrp).

You consent to (A)the use, copying, distribution, publication, modification and other processing of Registrant Personal Data by Donuts in a manner consistent with Donuts Inc. posted privacy policy (http://www.donuts.co/policies/privacy-policy/), and (B) Donuts reserves the right to deny, cancel or transfer any registration or transaction, or place any domain name(s) or other transactions on registry lock, hold or similar status, that it deems necessary, in its discretion; (a) to protect the integrity and stability of the Donuts TLD registries or the Registry System; (b) to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process; (c) to avoid any liability, civil or criminal, on the part of Donuts, as well as its affiliates, subsidiaries, officers, directors, and employees; (d) for violations of the Registrar-Registry Agreement; or (e) to correct mistakes made by Donuts or any Registrar in connection with a domain name registration. Donuts also reserves the right to place a domain name on registry hold, registry lock, or similar status during resolution of a dispute.

Feedback On the New Site? This site uses cookies to provide you with a better user experience. For more information, refer to our Privacy Policy Confirm

names in the same or other Donuts TLDs (e.g., renewal registration Fee is $7 for one domain name and $13 for a different domain name).

You acknowledge and agree that domains names are variably priced in the Donuts TLDs (i.e., some are Standard Names and others Premium Names), as described in the Registry Terms & Conditions.

Additional Provisions. You acknowledge and agree that You have reviewed and satisfied Yourself as to the obligations and conditions contained in the Registry Operator's policies, rules, guidelines, terms and conditions, and service agreement, including any subsequent amendments or modifications thereto ("Registry Operator's Policies"). You hereby agree to be bound by the Registry Operator's Policies. You further agree that You have a continuing obligation to periodically monitor such policies for any changes. Such Registry Operator's Policies may be found at the web site of the Registry Operator (located at http://www.donuts.co/policies/), and are incorporated herein.

Terms and conditions specific to Rightside Registry TLD domain registrations

1. By applying to register or reserve a domain name in a Registry TLD, you represent and warrant that neither your registration nor your use of the name will infringe the intellectual property or other rights of any third party or violate the Registry's Acceptable Use (Anti-Abuse) Policy.
2. You acknowledge and agree to abide by all Registry Policies set forth on the Registry's website at http://rightside.co/registry/for- registrars/#c290 (the "Registry Website"). You specifically acknowledge and agree that the Registry Policies may be modified by the Registry, and agree to comply with any such changes in the time period specified for compliance.
3. You agree to comply with all applicable ICANN requirements and policies found at www.icann.org/en/general/consensus-policies.htm.
4. You agree to comply with all applicable laws, including those that relate to privacy, data collection, consumer protection, fair lending, debt collection, organic farming, disclosure of date and financial disclosures.
5. You agree that should you use a Registry TLD to collect and or maintain sensitive health and financial data, you implement reasonable appropriate security measures commensurate with the offering of those services as defined by applicable law.
6. You represent and warrant that you have provided to your Registrar current, complete, and accurate information in connection with your application for a registration, and that you will correct and update this information to ensure that it remains current, complete, and accurate throughout the term of any resulting registration or reservation. Your obligation to provide current, accurate, and complete information is a material element of these terms, and the Registry reserves the right to deny, cancel, terminate, suspend, lock, or transfer any registration or reservation if it determines, in its sole discretion, that the information is materially inaccurate.
7. You consent to the collection, use, processing, and/or disclosure of personal information in the United States and in accordance with the Registry's Privacy Policy , and incorporated by reference here. If you are submitting information from a country other than the country in which the Registry servers are located, your communications with the Registry may result in the transfer of information (including your membership account information) across international boundaries; you consent to such transfer.
8. Should You choose to register one or more of these new generic top-level domain names, you must comply with the registration requirements as described below: Regulated TLDs: .ENGINEER, .MARKET, MORTGAGE, .DEGREE, .SOFTWARE, .VET, .GIVES, and .REHAB Highly-regulated TLDs: .DENTIST, .ATTORNEY, and .LAWYER Military TLDs: .ARMY, .NAVY, and .AIRFORCE.

    a. Safeguards for Regulated TLDs. Registrants must comply with all applicable laws, including those that relate to privacy, data collection, consumer protection (including in relation to misleading and deceptive conduct), fair lending, debt collection, organic farming, disclosure of data, and financial disclosures. Additionally, if a Registrant collects and maintains sensitive health and financial data, Registrants must implement reasonable and appropriate security measures commensurate with the offering of those services, as defined by applicable law.

    b. Safeguards for Highly-Regulated TLDs. Registrants must provide to their Registrar administrative contact information, which must be kept up-to-date, for the notification of complaints or reports of registration abuse, as well as the contact details of the relevant regulatory, or industry self-regulatory, bodies in their main place of business. Additionally, Registrants must possess any necessary authorizations, charters, licenses and/or other related credentials for participation in the sector associated with such Highly-regulated TLD and report any material changes to the Registrant's authorizations, charters, licenses and/or other related credentials for participation in the sector associated with the Highly-regulated TLD.

    c. Safeguards for Military TLDs. Registrant must take steps to ensure against misrepresenting or falsely implying that the Registrant or its business is affiliated with, sponsored or endorsed by one or more country's or government's military forces if such affiliation, sponsorship or endorsement does not exist.

9. You should be aware that Australian Defence Regulation 1957, No. 16, individuals and businesses, who are subject to Australian law, are prohibited from using the words "Navy"

Feedback On the New Site?
This site uses cookies to provide you with a better user experience. For more information, refer to our Privacy Policy
Confirm

selling or distributing any .NAVY or .AIRFORCE domain name.

10. You agree to submit to proceedings commenced under ICANN's Uniform Domain Name Dispute Resolution Policy ("UDRP"), and the Uniform Rapid Suspension System ("URS"), each as described on the ICANN Website. You further agree to abide by the final outcome of any of those processes, subject to any appeal rights provided in those processes or the law, and you hereby release the Registry, its affiliates and service providers from any and all directly or indirect liability associated with such dispute resolution processes.
11. You acknowledge and agree that the Registry reserves the right, in its sole discretion, to disqualify you or your agents from making or maintaining any registrations or reservations in the Registry TLD if you are found to have repeatedly engaged in abusive registrations.
12. You acknowledge and agree that the Registry reserves the right to deny, cancel, terminate, suspend, lock, or transfer any registration that it deems necessary, in its discretion, in furtherance of the following:

    a. to enforce all Registry Policies, these Registration Terms, and ICANN requirements, as amended from time to time;
    b. to protect the integrity and stability of the Registry, its operations, and the Registry TLDs;
    c. to comply with any applicable law, regulation, holding, order, or decision issued by a court, administrative authority, or dispute resolution service provider with jurisdiction over the Registry or you;
    d. to establish, assert, or defend the legal rights of the Registry or a third party, or to avoid any liability, civil or criminal, on the part of the Registry as well as its affiliates, subsidiaries, officers, directors, representatives, employees, contractors, and stockholders;
    e. to correct mistakes made by the Registry or any Registrar in connection with a registration or reservation;
    f. as otherwise provided herein.

13. The Registration Terms, its interpretation, and all disputes between the parties arising in any manner hereunder, shall be governed by and construed in accordance with the internal laws of the State of Washington, without giving effect to any choice or conflict of law provision or rule (whether of the State of Washington or any other jurisdiction). You agree and submit to the exercise of personal jurisdiction of courts in the State of Washington for the purpose of litigating any such claim or action.
14. BY AGREEING TO THESE REGISTRATION TERMS AND CONDITIONS, YOU ARE: (1) WAIVING CLAIMS THAT YOU MIGHT OTHERWISE HAVE AGAINST THE REGISTRY, ITS EMPLOYEES, AFFILIATES AND SUBSIDIARIES, AND SERVICE PROVIDERS, BASED ON THE LAWS OF OTHER JURISDICTIONS, INCLUDING YOUR OWN; (2) IRREVOCABLY CONSENTING TO THE EXCLUSIVE JURISDICTION OF, AND VENUE IN, STATE OR FEDERAL COURTS IN THE STATE OF WASHINGTON OVER ANY DISPUTES OR CLAIMS YOU HAVE WITH THE REGISTRY, ITS AFFILIATES AND SERVICE PROVIDERS; AND (3) SUBMITTING YOURSELF TO THE PERSONAL JURISDICTION OF COURTS LOCATED IN THE STATE OF STATE OF WASHINGTON FOR THE PURPOSE OF RESOLVING ANY SUCH DISPUTES OR CLAIMS.
15. You acknowledge and agree that the Registry is and shall be an intended third party beneficiary of the obligations you undertake under your registration agreement with the Registrar and these Registration Terms. You acknowledge and agree that the Registry's third party beneficiary rights have vested, and shall survive any termination or expiration of your registration or reservation.
16. You acknowledge and agree that domain names in the Registry TLD are provided "as is", "with all faults" and "as available." The Registry, its affiliates and service providers, make no express warranties or guarantees about such domain names.
17. TO THE GREATEST EXTENT PERMITTED BY LAW, THE REGISTRY, ITS AFFILIATES AND SERVICE PROVIDERS, DISCLAIM IMPLIED WARRANTIES THAT THE REGISTRY AND ALL SOFTWARE, CONTENT AND SERVICES DISTRIBUTED THROUGH THE REGISTRY, ITS AFFILIATES AND SERVICE PROVIDERS ARE MERCHANTABLE, OF SATISFACTORY QUALITY, ACCURATE, TIMELY, FIT FOR A PARTICULAR PURPOSE OR NEED, OR NON-INFRINGING. THE REGISTRY, ITS AFFILIATES AND SERVICE PROVIDERS DO NOT GUARANTEE THAT ANY REGISTRY TLDS, OR REGISTRY OPERATIONS WILL MEET YOUR REQUIREMENTS, WILL BE ERROR-FREE, RELIABLE, WITHOUT INTERRUPTION OR AVAILABLE AT ALL TIMES. WE DO NOT GUARANTEE THAT THE RESULTS THAT MAY BE OBTAINED FROM THE USE OF THE UNITED TLD, INCLUDING ANY SUPPORT SERVICES, WILL BE EFFECTIVE, RELIABLE, ACCURATE OR MEET YOUR REQUIREMENTS. WE DO NOT GUARANTEE THAT YOU OR THIRD PARTIES WILL BE ABLE TO ACCESS OR USE A DOMAIN NAME IN UNITED TLDS (EITHER DIRECTLY OR THROUGH THIRD-PARTY NETWORKS) AT TIMES OR LOCATIONS OF YOUR CHOOSING. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY A REPRESENTATIVE OF THE REGISTRY, ITS AFFILIATES AND SERVICE PROVIDERS SHALL CREATE A WARRANTY REGARDING OPERATIONS OF THE REGISTRY OR A DOMAIN NAME IN A REGISTRY TLD.
18. THE REGISTRY, ITS'AFFILIATES AND SERVICE PROVIDERS SHALL NOT BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES ARISING FROM YOUR USE OF, INABILITY TO USE, OR RELIANCE UPON A DOMAIN NAME IN A UNITED TLD. THESE EXCLUSIONS APPLY TO ANY CLAIMS FOR LOST PROFITS, LOST DATA, LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE

Feedback On the New Site?
This site uses cookies to provide you with a better user experience. For more information, refer to our Privacy Policy
Confirm

FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, IN SUCH STATES OR JURISDICTIONS, THE REGISTRY'S LIABILITY, AND THE LIABILITY OF THE REGISTRY'S AFFILIATES AND SERVICE PROVIDERS, SHALL BE LIMITED TO THE AMOUNT YOU PAID TO REGISTER A UNITED TLD. YOU FURTHER AGREE THAT IN NO EVENT SHALL THE REGISTRY'S, ITS AFFILIATES AND SERVICE PROVIDERS, TOTAL AGGREGATE LIABILITY EXCEED THE TOTAL AMOUNT PAID BY YOU FOR THE PARTICULAR SERVICES THAT ARE THE SUBJECT OF THE CAUSE OF ACTION. YOU AGREE THAT THE RIGHTS STATED HEREIN SURVIVE TERMINATION OF THE REGISTRAR'S AGREEMENT WITH YOU.

19. The Registry reserves the right to modify, change, or discontinue any aspect of its Registry Services, these Registration Terms, including without limitation its prices and fees. You acknowledge and agree that the Registry, its affiliates and service providers may provide any and all required notices, agreements, modifications and changes to these Registration Terms, and other information concerning Registry TLDs electronically, by posting such items on the Registry Website. Your continued use of a Registry TLD shall constitute your acceptance of the most current versions of those notices, agreements, modifications, and changes to these Registration Terms. In the event of any conflict between these Registration Terms and the notices, agreements, modifications and changes to the Registration Terms as posted from time to time on the Registry Website, the terms posted on the Registry Website shall prevail.
20. You represent and warrant that your use of the Registry and/or the Registry TLDs will not be for any illegal purpose and that you will not undertake any activities with your Registry TLD that will be in violation of the Acceptable Use (Anti-Abuse) Policy.
21. The Registry TLDs are intended for and available to applicants and registrants who are at least eighteen (18) years of age. By applying for, registering, or reserving United TLD, you represent and warrant that you are at least eighteen (18) years of age.

Terms and conditions specific .io, .ac and .sh domain registrations

You acknowledge and agree that You shall comply with the requirements, standards, policies, procedures and practices set forth in the nic.io Terms and Conditions, found here.

You further acknowledge that in utilizing our WHOIS privacy service you are specifically requesting that we enter information from our WHOIS privacy service in place of your information as the WHOIS contact details for your domain. Further, you are specifically agreeing and requesting that our privacy service will act as the offical Applicant agent for your domain per the nic.io terms linked to above.

Terms and conditions specific .osaka domain registrations

To register a domain name under the .OSAKA Top-Level Domain the Registrant (person or entity) must meet the Nexus Requirement. Eligible registrants include, but are not limited to:

- Osaka municipalities and local governments
- Public and private institutions in Osaka
- Organizations, companies, and other businesses/entities in Osaka
- Residents of Osaka
- Others who have a legitimate purpose for registering and using a [.osaka] domain

Terms and conditions specific .uk domain registrations

You acknowledge and agree that You shall comply with the requirements, standards, policies, procedures and practices set forth in the .uk Terms and Conditions, found here.

NameSilo
Domains. Cheap, easy and secure

There are less than 15 registrars in the world that have over 3 million active domains. We are proud to be one of them.

SHOPPING
Domains
Transfers
Marketplace
Pricing

ACCOUNT
Create Account
Login

SUPPORT
Support Catalog
Contact Us
WHOIS
Live Chat

BLOG

©2009-2022 NameSilo, LLC · All Rights Reserved.

Feedback On the New Site?
This site uses cookies to provide you with a better user experience. For more information, refer to our Privacy Policy
Confirm

Registration Agreement

Applicable from May 25, 2018

1. General

1. This agreement controls the rights and obligations between Key-Systems GmbH ("Registrar") and the domain holder or its agent or representative ("Customer") with regard to domain names that are registered and managed at the Registrar by the domain owner or on his behalf.

2. Customer is aware that Registrar is an official registrar for domains, accredited by the Internet Corporation for Assigned Names and Numbers (in the following ICANN) as well as by other national and international registries. In the provision of domain name registration or management services, Registrar acts as a mediator between the customer and the organizations responsible for the management of the central databases. Registrar has no influence on the fact that the domain names applied for the customers can be registered and/or are freely from third party rights. Registrar cannot guarantee for this and for the continued registration of the domain names.

3. The various top-level domains are administered by various different, national or private organizations ("registries"). ICANN and each of these organizations have their own terms and conditions regarding the registration and use of the domain names, and possibly proceedings regarding domain name disputes. Registrar is required to pass on these terms and policies and dispute policies to its customers. By requesting a domain registration or domain transfer, Customer declares to be aware of the existing and current registration terms and policies of ICANN and the respective registry and accepts them as an essential part of this agreement.

4. Customer further acknowledges that registration policies of the respective registries or ICANN policies may change from time to time and agrees to keep himself informed about the current rules and to either accept those changes or delete the affected domain names. Registrar will provide information on essential changes in its newsletters and will provide a link to the most current policies on its website.

5. Customer acknowledges that the registration of a domain name may be canceled at any time due to violation of applicable registry or Registrar policies. He agrees in particular to any cancellation, deletion or a transfer of the domain name in accordance with a condition or registration policy of the respective registry or due to an action of Registrar or the registry, provided that it is carried out by the Registrar or the registry operator (1) to correct errors at the registration or transfer, (2) to resolve disputes which concern the registered domain names or (3) due to a violation of the registration policies, provided that such action does not violate ICANN or registry policies.

6. Registrar may modify this registration agreement at any time. Registrar agrees to inform Customer of the change of the terms and conditions by mail or e-mail unless such notification requires unreasonable efforts. Customer can object to modifications within 14 days of the sending date of the notification. Should the Customer object, Registrar may choose to terminate the agreement within 14 days or at the next possible termination date. If Customer does not object, the new terms and conditions shall be regarded as accepted by Customer and shall become part of the contractual relationship.

7. If Customer registers a domain name for third parties or on their behalf, he must ensure before ordering that the third party knows and accepts all relevant policies and registration terms and conditions, including this registration agreement and our privacy policy. Customers who act as resellers or distributors are obliged to transmit these conditions completely and obligatory to the end customer/registrants and to document their approval by appropriate evidence. The customer is further required to inform the registrant about all notifications of the Registrar regarding their domain names, the registration terms and all fees applicable to the registration. The policies of the registries and ICANN applicable to Registrars apply accordingly for Customers acting as a reseller. Prior to requesting a termination of a domain name registration or change of registrant contact information, the authorization by the third party to request the termination or modification must be ensured. Transfer requests or requests for Transfer Codes by the third party must be treated in accordance with the transfer policies of the appropriate registry and/or ICANN. Customer undertakes to collect and maintain suitable evidence and required documentation as evidence of the customers agreement and prove the authorization for any actions performed on behalf of the third party by submitting these records to Registrar upon request.

8. If registered name holder registers a domain name through a third party, agent or distributor, he accepts all acts and omissions of these parties as his own. The registered name holder explicitly authorizes these parties to undertake administrative actions regarding all domain names registered on his behalf at Registrar.

9. Both Registrar as well as Customers authorized by registered name holder shall be considered designated agents of registered name holder with regard to the management and registration of a domain name with regard to ICANN, registry or other parties involved in the registration process.

10. In the event that Registrar, in accordance with the policies of the registry, can not maintain the registration of a domain name of Customer or its own accreditation, Registrar shall be entitled to an extraordinary termination of the registration agreement with Customer with a 14 days period to the end of month. As designated agent of the registered name holder, Registrar is at any time authorized to execute transactions deemed necessary for the management of a domain name including data updates or transfers.

2. Registration and transfers of domain names

1. By submitting a request for a registration and/or transfer a domain name by/to Registrar, Customer authorizes Registrar to transmit on his behalf all entries and modifications which he makes at Registrar (e.g. DNS Updates, Updates of registration data, other domain configurations) directly and in real time to the respective registry. Registrar is authorized to undo wrongful transactions.

2. Customer undertakes to guarantee that the applied-for domain name and the intended use of the domain name: (a) do not violate rights of third parties, (b) that there are no other legal or factual obstacles in conflict with the registration, (c) that the chosen name does not violate moral conventions, (d) that the registration request occurs in knowledge and consideration of the guidelines and policies of the relevant registry and (e) that he is authorized to request this operation. Registrar is not obliged to verify this authority. Registrar may reject any application to register or transfer of a domain name without reason.

3. Customer acknowledges that domain name registration requests are usually executed on a "first-come, first-served" principle by the registry. Registrar shall give no guarantee for a successful allocation of ordered domains and becomes free from the duty to perform the service in case of impossibility of the order. Registrar is not obliged to follow this principle in case of multiple requests for one domain name.

4. The registration term after the initial application for the registration of a domain name or the transfer of a domain name from another registrar can be between one and ten years, depending on the domain name.

5. By applying for a domain transfer from another provider to Registrar, Customer confirms that he is authorized to dispose over the domain name. After the transfer is completed the domain owner is obliged to review the accuracy of the data on record in the registration database for the domain name and to correct them if necessary. Registrar is authorized to undo domain name transfers in case a previous transfer of the domain name occurred without the authorization of a previous registrant of record, or in case control over the domain was unlawfully lost by a previous registrant of record.

6. By requesting a transfer of a domain name to a third party ("change of ownership"), Customer confirms that the third party has expressly agreed the change of ownership and the terms of this agreement and our privacy policy and will provide documentation to that effect upon request. Registrar is entitled to cancel or refuse to execute a change of ownership where such agreement is not documented.

7. Concerning registration of domain names in multilingual scripts (IDNs) or under newly introduced top-level domains, Registrar does not have any control of these registrations and it might be possible that the service will be modified, interrupted or even terminated by the registry without prior notice. Registrar has no obligation to guarantee the continuity of the existence or availability of domain names, their fitness for planned uses or applications and registration and use of such domain names is at the risk of Customer. Customer acknowledges that the functionality of domain names may not be the same as in regular domain names. Furthermore, Customer also acknowledges that a domain name may potentially not function fully or for each use as they may require necessary new technical features.

8. Customer expressly agrees to the immediate execution of the service by Registrar. The registration, the transfer and the renewal of a domain name is a service provided in accordance to Customer specifications. The right to withdraw from the agreement or to returns in distance contracts (§ 312 BGB) is therefore excluded.

2a. Premium Domain Names

For the presentation of this website and improvement of our service the use of cookies is necessary. For more information please review our cookie policy. I acknowledge having been notified. Ok

1. For domain names that have been designated by the respective registry as Premium Names special prices may apply for registration, renewal and/or transfers that differ from the standard pricing in a TLD („Premium Price"). In such cases, the respective fees for a transaction will be displayed separately.

2. Customer acknowledges and accepts that in case of an erroneous display of Premium Prices in the user interface at the time of registration, renewal or transfer of a Premium Domain Name Registrar may at any time undo the transaction and return the Premium Domain Name to the registry or the previous registrar, provided such display was caused by a missing or erroneous designation of the Premium Domain Name or the applicable fee by the registry, or if the designation as domain name was not recognized by Registrar. The prepaid fees for the transaction will be refunded to Customer. Alternatively, Registrar can offer maintaining the status of the transaction provided Customer pays the difference between the standard fee and the Premium Price.

3. In case a Registry changes a designation of a registered or requested domain name to Premium status, Registrar will inform Customer about such changes.

4. Transactions affecting Premium Domain Names that require a fee will only be performed after the applicable fee is received in full.

2b. Aftermarket Domain Names

1. Registrar allows the sale and purchase of domain names listed on aftermarket platforms. Such domain names may be listed either at fixed prices or with an invitation to make an offer during the domain search or on lists.

2. Customer acknowledges that aftermarket domain names are domain names already registered by third parties and that a Registrar transfer and the agreement of the current owner may be required prior to a domain name being available for use in the Customer account.

3. By making an offer to buy or by purchasing at a fixed price Customer authorizes Registrar to charge the appropriate amount in the Customer account.

4. Registrar cannot guarantee that an aftermarket domain name is still available at the time payment is received, that no higher offer is received or that the seller is authorized to dispose of the domain name. Customer agrees that Registrar may cancel orders that cannot be completed at the conditions of the order and may refund the payment as credit to the Customer account. Registrar is further authorized to retroactively cancel wrongful transfers.

5. Customer agrees to update the domain name ownership and other contact details immediately after being notified of the completion of a transaction.

6. In case of a charge back or other form of non-payment of a purchase price by Customer, Registrar is authorized to return the domain name to the sales provider or to assume ownership of the domain name.

7. Where Customer offers self-owned domain names on aftermarket platforms through Registrars' interface, Registrar is only responsible for the transmission of the placement request to the aftermarket provider. When placing a domain name on an aftermarket platform, Customer expressly authorizes Registrar to transfer the domain name to a new owner or agree to the transfer to another registrar when Registrar is requested to do so by the operator of the aftermarket platform. This authorization expires 60 days after the placement of the domain name and automatically renews for further 60 day terms upon expiration.

3. Domain owner data

1. The Customer is committed to provide Registrar with the following information and registration data for the purpose of documenting ownership and other authorizations, forwarding to the registry (if applicable) and possibly for the purpose of publishing in the public database of registered domain names. This processing occurs in full compliance with our privacy policy and applicable law. By providing or changing this data in the online interface, Customer assures that this information is correct, complete and truthful. This concerns in particular:
   - ✔ Current and complete information about the full name or name of a legal person, mailing address, e-mail address, voice telephone number;
   - ✔ The IP address of the domain name server (primary and secondary server) and the name of these servers;
   - ✔ The full name, postal address, e-mail address, voice telephone number of the administrative contact, the technical contact and the billing contact.

2. The necessary information and data may vary depending on the TLD. Depending on registry requirements or a registry, additional or less information may be required. As far as more data is required, this data must be provided during the registration process or alternatively delivered upon request by Registrar.

3. The information and data has to be updated when necessary, incomplete data must be completed. Customer acknowledges that the provision of incorrect, outdated or incomplete data can directly lead to loss of rights from the service without refund. This also applies in the event that Customer does not comply with any request of Registrar to correct the data or provide proof of its accuracy within a timely manner.

4. An update of the registered name holder data may trigger a temporary lock against transfer requests for the affected domain names. Where policy allows, Registrar may – but is not required to – offer an opt-out from this lock.

5. By providing data of a third party, Customer confirms that he has informed the third party about the provision and use of the data in the context of our privacy policy and that the third party has expressly agreed with this provision and use and is aware of these terms.

6. For the use of services intended to protect the privacy of data the policies and terms of the service provider apply. The same applies for trustee and local presence services.

4. Renewals of Registration

1. Renewals of registration are possible for 1 to 10 years depending on the domain name, provided the maximum registration term is not exceeded.

2. A contract for the registration and administration of a domain name shall be renewed automatically for another 12 month term at the end of the registration period if it is not terminated with a notice period of three months prior to the date of expiry, unless agreed otherwise.

3. For renewals the price list at the renewal date is applicable. The Customer acknowledges that renewal and transfer fees may change on a short notice and agreed to verify the current price prior to any order and any requested automatic renewal. As reasonably possible, Registrar will inform Customer about changes to the current fees in its newsletter. Registrar is authorized to cancel or modify orders if a price change occurs between the date of the order and the fulfillment date.

4. Customer will be informed by e-mail of his obligation to pay for the renewal in accordance with the provisions of ICANN or the respective registry in time before the end of the registration period. If Customer does not terminate the contract on time and Customer has either identified his payment method to be credit card or bank debit and entered current and valid payment details, then Registrar will automatically attempt to charge the due amount 10 days prior to the expiration date and the contract will be renewed accordingly. Customer is solely responsible for ensuring the timely receipt of the applicable fees or for the functionality of the chosen payment.

5. Termination of the management

1. In case the fee for a renewal of a registered domain name is not received 3 days before the expiry of the contract period, Customer loses his rights to the domain name. The same applies in the event of a charge back of a payment for a domain name or the selected payment method fails.

2. In the case of domain names canceled by the Customer, of domain names not extended at the time of expiry despite of a reminder of the pending expiration, or non-payment of renewal fees, Registrar is authorized to deactivate this domain name at its own discretion or to change the DNS entries ("deactivation"), to return it to the Registry for the purpose of deletion or continued management at the registry ("deletion") or to dispose, to auction, to transfer to third parties, to take over in his own continuance ("utilization"). Registrar will begin to undertake such actions no earlier than 14 days after the expiration of domain names with a Renewal Grace Period, or upon expiration of domain names without such a period. Customer agrees that the termination or non-renewal of the domain name or non-payment of due renewal fees shall constitute his consent to the actions described above as well as a renewal of the domain name to the extent necessary for their undertaking provided that Customer does not contradict expressly before the term end and no agreement to the contrary exists.

3. After the utilization of a domain names Registrar may in its own discretion to provide Customer with a share of the net proceeds of the utilization. The share will be credited to the customer account. For the purposes of this segment "net proceeds" shall mean the proceeds which the Registrar receives from another party or a third supplier as a result of the utilization, minus the costs linked to the utilization borne by Registrar. The customer agrees that no legal claim exists to any part of the net proceeds. Also Registrar makes no guarantee for the fact that any utilization will result in any net proceeds.

4. Regardless of the regulations here and in the general terms and conditions both sides can terminate the agreement for important reason.
   a. An important reason for Registrar is given in particular when Customer

For the presentation of this website and improvement of our service the use of cookies is necessary. For more information please review our cookie policy. I acknowledge having been notified. Ok

- is in more than 20 calendar-days delay of submitting the payment for a contract which has an undefined length;
- culpably violates duties of the contract, against ICANN or the registry policies or these registration terms, particularly by provision of false registration data;
- violates laws, rules or good morals with the content made available through the domain name or with the domain name itself, and despite warning and within reasonable time does not modify such content in such a way that they meet the requirements regulated herein, or
- acts contrary to terms and conditions of the registration or the registration policies.

b. Another important reason exists, if
- the accreditation of Registrar ends for a top-level domain under which the domain name is registered and the Registrar can not guarantee to continue the registration under the same conditions as well as when the registry terminates the operation of the top-level domain.

c. In these cases Customer loses all rights.

5. Customer may request transfers of his domain name to another provider. Registrar may refuse such a transfer request, subject to the conditions set by the registry or ICANN reasons for refusals of transfers. A transfer within 60 days of registration or a prior transfer or owner change is prohibited unless such transactions are expressly allowed by the registry.

6. Recovery and reactivation of domain names

1. If and as far as a registration authority permits the recovery ("Restore") of previously deleted domain names or domain names returned to the registry in certain TLDs and provided Registrar offers that service in the respective TLD, this service will be provided subject to change without notice at the request of the registered domain holder and with no guarantee of a successful Restore. The prices for this operation are defined in the price list and do not include renewal fees. A Restore can only be performed when the account has a sufficient balance for the operation and the domain name has been previously deleted. A Restore request can only be processed if it is received in time prior to the final deletion by the registry. In case a Restore cannot be executed the appropriate fees will be refunded to Customer's account.

2. As far as Registrar offers the reactivation of a deactivated domain name before a utilization, Customer agrees to pay the reactivation fees plus the cost of renewal for such orders.

7. Domain dispute policy

1. Customer agrees to resolve and settle any domain name dispute according to the Dispute Resolution Policies of the respective registry or ICANN, if applicable. These policies can be reviewed on the website of Registrar or on the website of the respective registry, or ICANN. Customer will inform himself about the applicable Dispute Resolution Policy before initiating a registration request. The language of the arbitration rules may be different from the language of the agreement and can be written in the local language of the registry.

2. Customer accepts that Registrar as an accredited registrar may be bound to lock or cancel a domain or to transfer it to a third party in accordance with any decision of an Administrative Panel in accordance with the applicable dispute resolution policy unless Customer provides evidence to Registrar within ten days after an Administrative Panel's decision that he has commenced a lawsuit against the complainant regarding the panel decision in a court of mutual jurisdiction.

3. For the adjudication of disputes concerning or arising from use of the Registered Name, the Registered Name Holder shall submit, without prejudice to other potentially applicable jurisdictions, to the jurisdiction of the courts (1) of the Registered Name Holder's domicile and (2) the legal domicile of Registrar.

4. During a pending administrative proceeding or during a period of 15 days after such proceeding is concluded or during a pending court proceeding or arbitration commenced regarding the domain name, Customer may not transfer the domain name registration to a third party unless the third party agrees, in writing, to be bound by the decision of the court or arbitrator.

8. Liability

1. As a condition of Customer's access and his use of the services of Registrar, Customer agrees to defend, indemnify, save and hold harmless Registrar, agents, partners, ICANN, the central registry as well as all persons involved in rendering of the service in respect to all claims, demands, liabilities, costs and/or expenses resulting from an illegal use of the service, of the domain name registered by Customer or the content provided on a registered domain. In the event of a claim, Customer has the right to prove Registrar, that claims in the context of the indemnity have not occurred in the extent demanded or not at all, and / or Customer is not responsible.

2. Neither Registrar, agents, partners, ICANN, the central registry nor any person involved in the rendering of the service will be liable to Customer or any third party for any direct or indirect loss of profits, earnings or business opportunities, damages, expense, or costs resulting directly or indirectly from any failure to perform any obligation or provide service hereunder because of any Force Majeure, or governmental acts or directives, strikes, riot or civil commotion, war, any natural disaster, equipment or facilities shortages which are being experienced by providers of telecommunication services generally, or other similar force or condition beyond Registrars reasonable control.

3. Registrar cannot be held liable for delays of services and server down times due to higher force, fault of third parties or due to events, which Registrar has no influence on, any agreed-upon deadlines and delivery dates non withstanding. Registrar may delay the provision of service and/or performance by the duration of the respective disruption plus an appropriate starting time. Furthermore, Registrar can limit access to the service, if the stability and security of the operation, the maintenance of the net integrity, in particular the avoidance of serious disturbances of the network, the software or stored data requires it. Registrar is not obligated to review or monitor the use of the service by Customer to ensure their legality.

4. For all services of Key-Systems´ liability will be limited to intent and gross negligence if and as much as it is legally permitted. In case of paid services liability is limited by KS with negligence and rough negligence to the amount of the payment which can be paid in each case from the Customer for the respective achievement and/or achievement period. For free and ancillary services the liability of Key-Systems is limited to cases of minor negligence and to an amount of 25 EURO for each single case or 100 EURO for all cases. In any other case the liability of Key-Systems is limited to typically foreseeable damages. Claims for punitive or consequential damages are excluded.

5. Customer shall compensate Registrar for any damages resulting from violations of the registration agreement, registration policies, and/or the terms and conditions and shall indemnify Registrar against all third-party claims based on the use of the services. This also includes the reimbursement of all reasonable costs of a legal defense if the Registrar or its employees was threatened with legal proceedings due to the registration or such proceeding are initiated.

6. This includes in particular the use of a domain name by infringing a prohibition in law, the good morals as well as rights of third parties (trademark rights, name rights, copy rights, data protection rights etc.) or the active support of such violations, making available of content that of glorifies violence, inciting, racist or radical right-wing content, the instructions for criminal acts and content that are appropriate to degrade a third party or group of third parties in their human dignity (hate-pages), the unauthorized intrusion into third party computers or computer systems, the distribution of malicious software, the distribution of illegal or regulated substances without the required authorizations, the forgery, the mailing of unrequested or undesirable e-mails for advertising purposes to third parties (Spamming). Customer is obliged to comply with all legal requirements and policies with the provision of pornographic and/or erotic content.

7. A registered domain name can be temporarily blocked or disabled if the Customer violates applicable law or this agreement in serious manner with the content made available under the domain name and Customer does not react to the request or Registrar to remove or modify the content accordingly. The same applies if such a violation is made plausible.

8. As far as a single domain name is canceled or transferred by Customer, or canceled due to violation of the registration agreement, due to binding decisions in domain name disputes or due to other causes specified in these conditions, no right to request for a free replacement domain or other reimbursement exists, provided that the termination was not caused illegally by Registrar in a culpable or grossly negligent manner. This also applies to other services or additionally booked options regarding the affected domain names.

9. Data sharing and data protection

1. Registrar advises Customer in accordance with the applicable data protection regulations of the fact that within the scope of the performance of the agreement personal data is collected, stored and processed and such data may be provided to third parties involved in the performance of the agreement. This also may include the provision of the data in freely accessible domain name registration databases. The registered name holder is hereby informed about the handling and processing of this data by Registrar and third parties involved in the provision of the service. The processing occurs on the basis of articles 6 I b)-f) of the GDRP. Further information on the specific acts of processing and their underlying legitimacy is included in the privacy policies of Registrar that are hereby incorporated

For the presentation of this website and improvement of our service the use of cookies is necessary. For more information please review our cookie policy. I acknowledge having been notified. Ok

2. Registrar is authorized to process and use Customer's data to improve the range of offered services according to the needs of its Customer.
3. Registrar is authorized to permanently store the data required for billing purposes in accordance with legal provisions.
4. In the event of police or other government requests, Registrar is authorized to transmit the data to such authorized requesting parties. The same applies to the transmission to third parties where they made plausible claims of violations of their rights.
5. Customer has the right to request information on his stored personal data at any time without charge.
6. Customer agrees that Registrar may send newsletters to his e-mail address for informational or marketing purposes. This consent may be revoked at any time.

10. Final clauses

1. Modifications or changes of terms or conditions or the contract, as well as cancellations will only be accepted in writing, for contract conclusions beginning from 2018-5-25 in text form – oral agreements shall not be considered valid. This also applies to terms and conditions of customers unless Registrar has expressly agreed to accept such terms in writing.
2. For commercial Customers and legal entities in Germany, as well as for all Customers without permanent residence in Germany, St. Ingbert/ Germany will be the exclusive place of jurisdiction for all disputes regarding services provided in accordance with this agreement. St. Ingbert, Germany shall also be the place of fulfillment.
3. For the contract between Registrar and Customers the German law is the only effective law. The United Nations Convention on Contracts for the International Sale of Goods shall not apply.
4. If any provision of this agreement – or parts thereof – contradict the terms, conditions, policies or other regulations of the relevant registries or ICANN, the provisions, terms, conditions, policies or other regulations of the relevant registries or ICANN shall apply instead.
5. If any provision of this agreement shall be or become unenforceable and/or invalid, such unenforceability and/or invalidity shall not render this agreement unenforceable or invalid as a whole. Any provision determined to be unenforceable or invalid shall be replaced by provisions which are valid and enforceable and closest to the original objectives and intents of the original provisions in an economic and legal sense that would have been agreed upon by the parties, had they known of the invalidity at the time of the agreement. As far as legally possible, Registrar shall replace the clause in the above mentioned extent.
6. Both, the English and German version of this agreement are valid and binding. In case of doubt or conflict, however, the German version will prevail.

For the presentation of this website and improvement of our service the use of cookies is necessary. For more information please review our cookie policy. I acknowledge having been notified. Ok

Exhibit 8

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

MICROSOFT CORPORATION, a Washington corporation,

Plaintiff,

v.

JOHN DOES 1-2 CONTROLLING A COMPUTER NETWORK AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS

Defendants.

Case: 1:19-cv-00716 (JURY-DEMAND)
Assigned To : Amy B. Jackson
Assign. Date : 3/14/2019
Description: TRO/PI

FILED UNDER SEAL PURSUANT TO LOCAL RULE 5.1

FILED
MAR 15 2019
Clerk, U.S. District & Bankruptcy Courts for the District of Columbia

EX PARTE TEMPORARY RESTRAINING ORDER AND
ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

Plaintiff Microsoft Corp. ("Microsoft") has filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) the Electronic Communications Privacy Act (18 U.S.C. § 2701); (3) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); (4) the Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)); and (5) the common law of trespass to chattels, unjust enrichment, conversion, intentional interference with contractual relationships, and unfair competition. Microsoft has moved ex parte for an emergency temporary restraining order and an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C. § 1116(a) (the Lanham Act), and 28 U.S.C. § 1651(a) (the All-Writs Act).

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Microsoft's Application for an Emergency Temporary Restraining Order, the Court hereby

makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case, and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against Defendants John Doe 1 and 2 ("Defendants") under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), the Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)), and common law of trespass to chattels, unjust enrichment, conversion, intentional interference with contractual relationships, and unfair competition.

2. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)) and constitute common law of trespass to chattels, unjust enrichment, conversion, and tortious interference with prospective and actual business relations, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. Microsoft owns the registered trademarks "Microsoft," "Windows Live," "Office 365," "Outlook," "Hotmail" and "OneDrive" used in connection with its services, software and products.

4. There is good cause to believe that, unless Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations. The evidence set forth in Microsoft's Brief in Support of Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO

Application"), and the accompanying declarations and exhibits, demonstrates that Microsoft is likely to prevail on its claim that Defendants have engaged in violations of the foregoing law by:

a. intentionally accessing and sending malicious software, code, and instructions to the protected computers, operating systems, and computer networks of Microsoft and the customers of Microsoft, without authorization or exceeding authorization, in order to

   i. infect those computers and computer networks with malicious code and thereby gain control over those computers and computer networks;

   ii. attack and compromise the security of those computers and computer networks by conducting remote reconnaissance, stealing authentication credentials, monitoring the activities of users, and using other instrumentalities of theft;

   iii. steal and exfiltrate information from those computers and computer networks;

b. deploying computers and Internet domains to establish a command and control infrastructure by which means Defendants conduct illegal activities, including attacks on computers and networks, monitoring activities of users, and theft of information;

c. corrupting Microsoft's operating system and applications on victims' computers and networks, thereby using them to monitor the activities of users and steal information from them;

5. There is good cause to believe that if such conduct continues, irreparable harm will occur to Microsoft, Microsoft's customers, and the public. There is good cause to believe that the Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court;

6. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of command and control software that is hosted at and otherwise operates through the Internet domains listed in **Appendix A** to the Complaint and from the destruction or concealment of other discoverable evidence of Defendants' misconduct

available via those domains, including on user computers infected by Defendants, if Defendants receive advance notice of this action. Based on the evidence cited in Microsoft's TRO Application and accompanying declarations and exhibits, Microsoft is likely to be able to prove that:

a. Defendants are engaged in activities that directly violate United States law and harm Microsoft and the public, including Microsoft's customers;

b. Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests;

c. Defendants are likely to delete or to relocate the command and control software at issue in Microsoft's TRO Application and the harmful and malicious software disseminated through the Internet domains listed in Appendix A, thereby permitting them to continue their illegal acts; and

7. Microsoft's request for this emergency ex parte relief is not the result of any lack of diligence on Microsoft's part, but instead based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), 15 U.S.C. § 1116(a) and 28 U.S.C. § 1651(a), good cause and the interest of justice require that this Order be Granted without prior notice to Defendants, and accordingly, Microsoft is relieved of the duty to provide Defendants with prior notice of Microsoft's motion.

8. There is good cause to believe that Defendants have specifically directed their activities to computers of Microsoft's customers located in the District of Columbia, have engaged in illegal activity using the Internet domains identified in **Appendix A** to the Complaint by directing malicious code and content to said computers of Microsoft's customers to further perpetrate their illegal conduct victimizing Microsoft's customers. There is good cause to believe that Defendants have directed said malicious code and content through certain instrumentalities – specifically the domains and the domain registration facilities of the domain registries identified in **Appendix A**.

9. There is good cause to believe that Defendants have engaged in illegal activity by using the domain registration facilities of the domain registries identified in **Appendix A** to register the Internet domains identified in **Appendix A**, so as to deliver from those domains the malicious code, content, and commands that Defendants use to access Microsoft's services without authorization and to infect and compromise the computers of Microsoft's customers, and to receive the information stolen from those computers.

10. There is good cause to believe that Defendants have engaged in illegal activity by using deceptive and fake methods to steal computer users' login and/or account credentials and to use such credentials for illegal purposes.

11. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants must be prohibited from accessing Microsoft's services without authorization and prohibited from sending malicious code, content and commands from the Internet domains identified in **Appendix A** to the computers of Microsoft's customers.

12. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains identified in **Appendix A** to host the command and control software and content used to infect and compromise the computers and networks of Microsoft's customers and to steal information from them. There is good cause to believe that to immediately halt the injury caused by Defendants, each of Defendants' current and prospective domains set forth in **Appendix A** must be immediately redirected to the Microsoft-secured name-servers named NS149.microsoftinternetsafety.net and NS150.microsoftinternetsafety.net, thus making them inaccessible to Defendants for command and control purposes.

13. There is good cause to believe that to immediately halt the injury, the execution of this Order should be carried out in a coordinated manner by Microsoft and by the domain

registries identified in **Appendix A** on such date and time within ten days of this Order as may be reasonably requested by Microsoft.

14. There is good cause to believe that Defendants may change the Internet domains that they use to conduct illegal activities, and that Microsoft may identify and update the domains listed in **Appendix A** as may be reasonably necessary to account for additional Internet domains associated with Defendants just prior to the execution of this Order and within a reasonable time thereafter should Defendants attempt to evade and defy this Order.

15. There is good cause to permit notice of the instant Order, notice of the Preliminary Injunction hearing and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, and satisfy Fed. R. Civ. P. 4(f)(3) and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to Defendants' domain registrars and hosting companies and as agreed to by Defendants in Defendants' domain registration and/or hosting agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent Defendants provided accurate contact information in the U.S.; and (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Defendants, to the extent Defendants provided accurate contact information in foreign countries that are signatories to such treaties.

TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

IT IS THEREFORE ORDERED that, Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants, are temporarily restrained

and enjoined from: (1) intentionally accessing and sending malicious software or code to Microsoft and the protected computers and operating systems of Microsoft and Microsoft's customers, without authorization, in order to infect those computers; (2) intentionally attacking and compromising computers or computer networks of Microsoft or Microsoft's customers, to monitor the activities of the owners or users of those computers or computer networks, and to steal information from those computers or networks; (3) configuring, deploying, operating, or otherwise participating in or facilitating a command and control infrastructure described in the TRO Application, including but not limited to the command and control software hosted at and operating through the Internet domains set forth in **Appendix A** and through any other component or element of the command and control infrastructure at any location; (4) stealing information from Microsoft's customers; (5) misappropriating that which rightfully belongs to Microsoft, its customers, or in which Microsoft or its customers have a proprietary interest; (6) downloading or offering to download additional malicious software onto the computers of Microsoft's customers; or (7) undertaking any similar activity that inflicts harm on Microsoft, Microsoft's customers, or the public.

IT IS FURTHER ORDERED that, Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants are temporarily restrained and enjoined from (1) using and infringing Microsoft's trademarks, including specifically Microsoft's registered trademark "Microsoft," bearing registration number 5449084, "Hotmail," bearing registration number 2165601, "Outlook," bearing registration number 4255129, "Windows Live," bearing registration number 3765517, "OneDrive," bearing registration number 4941897, "OneDrive," bearing registration number 4661770, "OneDrive," bearing registration number 4827884, "Office 365," bearing registration number 4380754, and/or other

trademarks, trade names, service marks, or Internet Domain addresses or names; (2) using in connection with Defendants' activities, products, or services any false or deceptive designation, representation or description of Defendants or of their activities, whether by symbols, words, designs or statements, which would damage or injure Microsoft or give Defendants an unfair competitive advantage or result in deception of consumers; or (3) acting in any other manner which suggests in any way that Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Microsoft, or passing off Defendants' activities, products or services as Microsoft's.

IT IS FURTHER ORDERED that, with respect to any currently registered Internet domains set forth in **Appendix A**, the domain registries shall take the following actions:

A. Within five (5) business days of receipt of this Order, shall unlock and change the registrar of record for the domain to MarkMonitor or such other registrar specified by Microsoft. To the extent the registrar of record does not assist in changing the registrar of record for the domain under its control, the domain registry for the domain, or its administrators, including backend registry operators or administrators, within five (5) business days of receipt of this Order, shall change, or assist in changing, the registrar of record for the domain to MarkMonitor or such other registrar specified by Microsoft. The purpose of this paragraph is to ensure that Microsoft has control over the hosting and administration of the domain in its registrar account at MarkMonitor or such other registrar specified by Microsoft. Microsoft shall provide to the domain registry or registrar of record any requested registrar information or account details necessary to effectuate the foregoing.

B. The domain shall be made active and shall resolve in the manner set forth in this order, or as otherwise specified by Microsoft, upon taking control of the domain;

C. The domain shall be redirected to secure servers by changing the authoritative name servers to NS151.microsoftinternetsafety.net and NS152.microsoftinternetsafety.net and, as may be necessary, the IP addresses associated with name servers or taking other reasonable steps to work with Microsoft to ensure the redirection of the domain and to ensure that Defendants cannot use it to make unauthorized access to computers, infect computers, compromise computers and computer networks, monitor the owners and users of computers and computer networks, steal information from them or engage in any other activities prohibited by the Injunction;

D. The WHOIS registrant, administrative, billing and technical contact and identifying information should be the following, or other information as may be specified by Microsoft:

Domain Administrator
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
United States
Phone: +1.4258828080
Facsimile: +1.4259367329
domains@microsoft.com

E. Prevent transfer, modification or deletion of the domain by Defendants and prevent transfer or control of the domain to the account of any party other than Microsoft;

F. Take all steps required to propagate to the foregoing changes through the Domain Name System ("DNS"), including domain registrars.

IT IS FURTHER ORDERED that copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint may be served by any means authorized by law, including (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to Defendants' domain registrars and/or hosting companies

and as agreed to by Defendants in the domain registration and/or hosting agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent Defendants provided accurate contact information in the U.S.; and (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Defendants, to the extent Defendants provided accurate contact information in foreign countries that are signatories to such treaties.

IT IS FURTHER ORDERED, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before this Court on April 3, 2019 at 10:00 AM to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against Defendants, enjoining Defendants from the conduct temporarily restrained by the preceding provisions of this Order.

IT IS FURTHER ORDERED that Microsoft shall post bond in the amount of $50,000 to be paid into the Court registry.

IT IS FURTHER ORDERED that Microsoft may identify and update the domains in **Appendix A** to the Complaint as may be reasonably necessary to account for additional Internet domains associated with Defendants' illegal conduct just prior to or within a reasonable time after the execution of this Order.

IT IS FURTHER ORDERED that Defendants shall file with the Court and serve on Microsoft's counsel any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later than one (1) day prior to the hearing on Microsoft's request for a preliminary injunction.

IT IS SO ORDERED

Entered this 15th day of March, 2019

11:18 a.m.

UNITED STATES DISTRICT JUDGE

Exhibit 9

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

MICROSOFT CORPORATION, a Washington corporation, Plaintiff, v. JOHN DOES 1-2 CONTROLLING A COMPUTER NETWORK THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS, Defendants.	Civil Action No: **FILED UNDER SEAL PURSUANT TO LOCAL CIVIL RULE 5**

***EX PARTE* TEMPORARY RESTRAINING ORDER AND**
ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

Plaintiff Microsoft Corporation ("Microsoft") has filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) the Electronic Communications Privacy Act (18 U.S.C. § 2701); (3) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); (4) the Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)); and (5) the common law of trespass to chattels, unjust enrichment, conversion and intentional interference with contractual relationships. Microsoft has moved *ex parte* for an emergency temporary restraining order and an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C. § 1116(a) (the Lanham Act), and 28 U.S.C. § 1651(a) (the All-Writs Act).

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Microsoft's *Ex Parte* Application for an Emergency Temporary Restraining Order and Order to

Show Cause re Preliminary Injunction, the Court hereby makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case, and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against Defendants John Doe 1 and 2 ("Defendants") under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), the Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)), and common law of trespass to chattels, unjust enrichment, conversion, and intentional interference with contractual relationships.

2. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), the Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)) and constitute common law of trespass to chattels, unjust enrichment, conversion, and intentional interference with contractual relationships, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. Microsoft owns the registered trademarks Microsoft, Windows, Hotmail, Outlook, and Office 365 and numerous other trademarks used in connection with its services, software and products. There is good cause to believe that, unless Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations. The evidence set forth in Microsoft's Brief in Support of *Ex Parte* Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Application"), and the accompanying declarations and exhibits, demonstrates

that Microsoft is likely to prevail on its claim that Defendants have engaged in violations of the foregoing law by:

a. intentionally accessing and sending malicious software, code, and instructions to the protected computers, operating systems, and computer networks of Microsoft and the customers of Microsoft, without authorization or exceeding authorization, in order to

   i. steal and exfiltrate information from those computers and computer networks;

   ii. infect those computers and computer networks with malicious code and thereby gain control over those computers and computer networks;

   iii. attack and compromise the security of those computers and computer networks by conducting remote reconnaissance, stealing authentication credentials, monitoring the activities of users, and using other instrumentalities of theft;

b. deploying computers and Internet domains to establish a command and control infrastructure by which means Defendants conduct illegal activities, including attacks on computers and networks, monitoring activities of users, and theft of information;

c. corrupting Microsoft's operating system and applications on victims' computers and networks, thereby using them to monitor the activities of users and steal information from them;

4. There is good cause to believe that if such conduct continues, irreparable harm will occur to Microsoft, Microsoft's customers, and the public. There is good cause to believe that the Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court.

5. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of command and control software that is hosted at and otherwise operates through the Internet domains listed in **Appendix A** to the Complaint and from the destruction or concealment of other discoverable evidence of Defendants' misconduct

available via those domains, including on user computers infected by Defendants, if Defendants receive advance notice of this action. Based on the evidence cited in Microsoft's TRO Application and accompanying declarations and exhibits, Microsoft is likely to be able to prove that:

a. Defendants are engaged in activities that directly violate United States law and harm Microsoft and the public, including Microsoft's customers;

b. Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests;

c. Defendants are likely to delete or to relocate the command and control software at issue in Microsoft's TRO Application and the harmful and malicious software disseminated through the Internet domains listed in **Appendix A** to the Complaint, thereby permitting them to continue their illegal acts; and

d. Defendants are likely to warn their associates engaged in such activities if informed of Microsoft's action.

6. Microsoft's request for this emergency *ex parte* relief is not the result of any lack of diligence on Microsoft's part, but instead based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), 15 U.S.C. § 1116(a) and 28 U.S.C. § 1651(a), good cause and the interest of justice require that this Order be Granted without prior notice to Defendants, and accordingly, Microsoft is relieved of the duty to provide Defendants with prior notice of Microsoft's motion.

7. There is good cause to believe that Defendants have specifically directed their activities to computers of Microsoft's customers located in Virginia and the Eastern District of Virginia, have engaged in illegal activity using the Internet domains identified in **Appendix A** to the Complaint by using those domains to deceive users of Microsoft's products and services and by directing malicious code and content to said computers of Microsoft's customers to further perpetrate their illegal conduct victimizing Microsoft's customers. There is good cause

to believe that Defendants have directed said malicious code and content through certain instrumentalities – specifically the domains and the domain registration facilities of the domain registries identified in **Appendix A** to the Complaint.

8. There is good cause to believe that Defendants have engaged in illegal activity by using the domain registration facilities of the domain registries identified in **Appendix A** to the Complaint to register the Internet domains identified in **Appendix A**, so as to deceive Microsoft's customers to steal credentials for their Microsoft accounts, and to deliver from those domains the malicious code, content, and commands that Defendants use to access Microsoft's services without authorization and to infect and compromise the computers of Microsoft's customers, and to receive the information stolen from those accounts and computers.

9. There is good cause to believe that Defendants have engaged in illegal activity by using deceptive and fraudulent methods to steal computer users' account credentials and to use such credentials for illegal purposes.

10. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants must be prohibited from accessing Microsoft's services without authorization and prohibited from sending malicious code, content and commands from the Internet domains identified in **Appendix A** to the Complaint to the computers of Microsoft's customers.

11. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains identified in **Appendix A** to the Complaint to host the command and control software and content used to infect and compromise the computers and networks of Microsoft's customers and to steal information from them. There is good cause to believe that to immediately halt the injury caused by Defendants, each of Defendants' current and

prospective domains set forth in **Appendix A** to the Complaint must be immediately redirected to the Microsoft-secured name-servers named NS151.microsoftinternetsafety.net and NS152.microsoftinternetsafety.net, thus making them inaccessible to Defendants for command and control purposes.

12. There is good cause to believe that to immediately halt the injury, the execution of this Order should be carried out in a coordinated manner by Microsoft and by the domain registries identified in **Appendix A** to the Complaint on such date and time within five (5) days of this Order as may be reasonably requested by Microsoft.

13. There is good cause to believe that Defendants may change the Internet domains that they use to conduct illegal activities, and that Microsoft may identify and update the domains listed in **Appendix A** to the Complaint as may be reasonably necessary to account for additional Internet domains associated with Defendants just prior to the execution of this Order and within a reasonable time thereafter should Defendants attempt to evade and defy this Order.

14. There is good cause to permit notice of the instant Order, notice of the Preliminary Injunction hearing and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, and satisfy Fed. R. Civ. P. 4(f)(3) and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to Defendants' domain registrars and hosting companies and as agreed to by Defendants in Defendants' domain registration and/or hosting agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent Defendants provided accurate contact information in the

U.S.; and (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Defendants, to the extent Defendants provided accurate contact information in foreign countries that are signatories to such treaties.

TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

IT IS THEREFORE ORDERED that, Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants, are temporarily restrained and enjoined from: (1) intentionally accessing and sending malicious software or code to Microsoft and the protected computers and operating systems of Microsoft and Microsoft's customers, without authorization, in order to infect those computers; (2) intentionally attacking and compromising computers or computer networks of Microsoft or Microsoft's customers, to monitor the activities of the owners or users of those computers or computer networks, and to steal information from those computers or networks; (3) configuring, deploying, operating, or otherwise participating in or facilitating a command and control infrastructure described in the TRO Application, including but not limited to the command and control software hosted at and operating through the Internet domains set forth in **Appendix A** to the Complaint and through any other component or element of the command and control infrastructure at any location; (4) stealing information from Microsoft's customers; (5) misappropriating that which rightfully belongs to Microsoft, its customers, or in which Microsoft or its customers have a proprietary interest; (6) downloading or offering to download additional malicious software onto the computers of Microsoft's customers; or (7) undertaking any similar activity that inflicts harm on Microsoft, Microsoft's customers, or the public.

IT IS FURTHER ORDERED that, Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants are temporarily restrained and

enjoined from (1) using and infringing Microsoft's trademarks, including specifically Microsoft's registered trademarks Microsoft, Windows, Hotmail, Outlook, and Office 365 and/or other trademarks, trade names, service marks, or Internet Domain addresses or names containing or infringing such trademarks, trade names or service marks; (2) using in connection with Defendants' activities, products, or services any false or deceptive designation, representation or description of Defendants or of their activities, whether by symbols, words, designs or statements, which would damage or injure Microsoft or give Defendants an unfair competitive advantage or result in deception of consumers; or (3) acting in any other manner which suggests in any way that Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Microsoft, or passing off Defendants' activities, products or services as Microsoft's.

IT IS FURTHER ORDERED that, with respect to any currently registered Internet domains set forth in **Appendix A** to this Order and the Complaint, the domain registries shall take the following actions:

A. Within five (5) business days of receipt of this Order, shall unlock and change the registrar of record for the domain to MarkMonitor or such other registrar specified by Microsoft. To the extent the registrar of record does not assist in changing the registrar of record for the domain under its control, the domain registry for the domain, or its administrators, including backend registry operators or administrators, within five (5) business days of receipt of this Order, shall change, or assist in changing, the registrar of record for the domain to MarkMonitor or such other registrar specified by Microsoft. The purpose of this paragraph is to ensure that Microsoft has control over the hosting and administration of the domain in its registrar account at MarkMonitor or such other registrar specified by Microsoft. Microsoft shall

provide to the domain registry or registrar of record any requested registrar information or account details necessary to effectuate the foregoing.

B. The domain shall be made active and shall resolve in the manner set forth in this order, or as otherwise specified by Microsoft, upon taking control of the domain;

C. The domain shall be redirected to secure servers by changing the authoritative name servers to NS096A.microsoftinternetsafety.net and NS096B.microsoftinternetsafety.net and, as may be necessary, the IP addresses associated with name servers or taking other reasonable steps to work with Microsoft to ensure the redirection of the domain and to ensure that Defendants cannot use it to make unauthorized access to computers, infect computers, compromise computers and computer networks, monitor the owners and users of computers and computer networks, steal information from them or engage in any other activities prohibited by the Injunction;

D. The WHOIS registrant, administrative, billing and technical contact and identifying information should be the following, or other information as may be specified by Microsoft:

Domain Administrator
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
United States
Phone: +1.4258828080
Facsimile: +1.4259367329
domains@microsoft.com

E. Prevent transfer, modification or deletion of the domain by Defendants and prevent transfer or control of the domain to the account of any party other than Microsoft;

F. Take all steps required to propagate to the foregoing changes through the Domain Name System ("DNS"), including domain registrars.

IT IS FURTHER ORDERED that copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint may be served by any means authorized by law, including (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to Defendants' domain registrars and/or hosting companies and as agreed to by Defendants in the domain registration and/or hosting agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent Defendants provided accurate contact information in the U.S.; and (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Defendants, to the extent Defendants provided accurate contact information in foreign countries that are signatories to such treaties.

IT IS FURTHER ORDERED, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before this Court on Jan 3, 2020 at 10:00 am to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against Defendants, enjoining Defendants from the conduct temporarily restrained by the preceding provisions of this Order.

IT IS FURTHER ORDERED that Microsoft shall post bond in the amount of $50,000 to be paid into the Court registry.

IT IS FURTHER ORDERED that Microsoft may identify and update the domains in **Appendix A** to this Order and the Complaint as may be reasonably necessary to account for additional Internet domains associated with Defendants' illegal conduct just prior to or within a reasonable time after the execution of this Order.

IT IS FURTHER ORDERED that Defendants shall file with the Court and serve on Microsoft's counsel any answering affidavits, pleadings, motions, expert reports or

declarations and/or legal memoranda no later than one (1) day prior to the hearing on Microsoft's request for a preliminary injunction.

IT IS SO ORDERED

Entered this 18th day of December, 2019

2:10 pm

/s/ LOG
UNITED STATES DISTRICT JUDGE
United States District Judge

Exhibit 10

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

SOPHOS LIMITED, a United Kingdom limited company, and SOPHOS INC., a Massachusetts corporation, Plaintiffs, v. JOHN DOES 1-2, Defendants.	Civil Action No: 1:20cv502 **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5**

***EX PARTE* TEMPORARY RESTRAINING ORDER AND**
ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

Plaintiffs Sophos Limited and Sophos Inc. (collectively, "Sophos") have filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) Trademark Infringement under the Lanham Act, 15 U.S.C. § 1114 *et seq.*; (3) False Designation of Origin under the Lanham Act, 15 U.S.C. § 1125(a); (4) Trademark Dilution under the Lanham Act, 15 U.S.C. § 1125(c); and (5) Unjust Enrichment. Sophos has moved *ex parte* for an emergency temporary restraining order and an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C. § 1116(a) (the Lanham Act), and 28 U.S.C. § 1651(a) (the All Writs Act).

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Sophos's *Ex Parte* Application for an Emergency Temporary Restraining Order and Order to Show Cause re Preliminary Injunction, the Court hereby makes the following findings of fact

and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case, and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against Defendants John Doe 1 and 2 ("Defendants") under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Lanham Act (15 U.S.C. §§ 1114, 1125), the Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)), and common law of unjust enrichment.

2. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Lanham Act (15 U.S.C. §§ 1114, 1125), the Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)) and constitute common law unjust enrichment, and that Sophos is, therefore, likely to prevail on the merits of this action;

3. Sophos owns the registered trademark "Sophos" used in connection with its services, software and products. There is good cause to believe that, unless Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations. The evidence set forth in Sophos's Brief in Support of *Ex Parte* Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Application"), and the accompanying declarations and exhibits, demonstrates that Sophos is likely to prevail on its claim that Defendants have engaged in violations of the foregoing law by:

   a. intentionally accessing and sending malicious software, code, and instructions to the protected computers and operating systems of Sophos, without authorization or exceeding authorization, in order to

      i. infect those computers and operating systems with malicious code and thereby attempt to gain control over those computers and operating systems;

ii. attack the security of those computers by conducting remote reconnaissance, and attempting to access information on those computers, without authorization;

b. deploying computers and Internet domains to establish a command and control infrastructure by which means Defendants conduct the foregoing illegal activities;

4. There is good cause to believe that if such conduct continues, irreparable harm will occur to Sophos. There is good cause to believe that the Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court.

5. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of command and control software that is hosted at and otherwise operates through the Internet domains listed in **Appendix A** to this Order and from the destruction or concealment of other discoverable evidence of Defendants' misconduct available via those domains, including on user computers infected by Defendants, if Defendants receive advance notice of this action. Based on the evidence cited in Sophos's TRO Application and accompanying declarations and exhibits, Sophos is likely to be able to prove that:

a. Defendants are engaged in activities that directly violate United States law and harm Sophos;

b. Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests;

c. Defendants are likely to delete or to relocate the command and control software at issue in Sophos's TRO Application and the harmful and malicious software disseminated through the Internet domains listed in **Appendix A** to this Order, thereby permitting them to continue their illegal acts; and

d. Defendants are likely to warn their associates engaged in such activities if informed of Sophos's action.

6. Sophos's request for this emergency *ex parte* relief is not the result of any lack of

diligence on Sophos's part, but instead based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), 15 U.S.C. § 1116(a) and 28 U.S.C. § 1651(a), good cause and the interest of justice require that this Order be Granted without prior notice to Defendants, and accordingly, Sophos is relieved of the duty to provide Defendants with prior notice of Sophos's motion.

7. There is good cause to believe that Defendants have specifically directed their activities to Sophos's firewall devices located in Virginia, including in the vicinity of Alexandria, Virginia, and the Eastern District of Virginia, have engaged in illegal activity using the Internet domains identified in **Appendix A** to this Order by using those domains to direct malicious code to Sophos's firewall devices to further perpetrate their illegal conduct. There is good cause to believe that Defendants have directed said malicious code and content through certain instrumentalities—specifically the domains and the domain registration facilities of the domain registries identified in **Appendix A** to this Order.

8. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants must be prohibited from accessing Sophos's firewall devices without authorization and prohibited from sending malicious code, content and commands from the Internet domains identified in **Appendix A** to this Order to Sophos's firewall devices.

9. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains identified in **Appendix A** to this Order to host the command and control software used to deliver malicious software to Sophos's firewall devices. There is good cause to believe that to immediately halt the injury caused by Defendants, each of Defendants' current and prospective domains set forth in **Appendix A** to this Order must be immediately transferred to the control of Sophos, thus making them inaccessible to Defendants for command

and control purposes.

10. There is good cause to believe that to immediately halt the injury, the execution of this Order should be carried out in a coordinated manner by Sophos and by the domain registries identified in **Appendix A** to this Order on such date and time within five (5) days of this Order as may be reasonably requested by Sophos.

11. There is good cause to believe that Defendants may change the Internet domains that they use to conduct illegal activities, and that Sophos may identify and update the domains listed in **Appendix A** to this Order as may be reasonably necessary to account for additional Internet domains associated with Defendants just prior to the execution of this Order and within a reasonable time thereafter should Defendants attempt to evade and defy this Order.

12. There is good cause to permit notice of the instant Order, notice of the Preliminary Injunction hearing and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, and satisfy Fed. R. Civ. P. 4(f)(3) and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to Defendants' domain registrars and hosting companies and as agreed to by Defendants in Defendants' domain registration and/or hosting agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent Defendants provided accurate contact information in the U.S.; and/or (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Defendants, to the extent Defendants provided accurate contact information in foreign countries that are signatories to such treaties.

TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

IT IS THEREFORE ORDERED that, Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants, are temporarily restrained and enjoined from: (1) intentionally accessing and sending malicious software or code to Sophos's protected computers, including its firewall devices, or the computers or networks of any other party, without authorization; (2) intentionally attacking and compromising computers of Sophos, including its firewall devices, or the computers or networks of any other party, to access computing resources and information on those devices, or for any other illegal purpose; (3) configuring, deploying, operating, or otherwise participating in or facilitating a command and control infrastructure described in the TRO Application, including but not limited to the command and control software hosted at and operating through the Internet domains set forth in **Appendix A** to this Order and through any other component or element of the command and control infrastructure at any location; (4) stealing information from Sophos or any other party, including through the foregoing activities; (5) misappropriating that which rightfully belongs to Sophos or any other party, or in which Sophos or any other party has a proprietary interest, including through the foregoing activities; (6) downloading or offering to download additional malicious software onto Sophos's firewalls or the computer of any other party; or (7) undertaking any similar activity that inflicts harm on Sophos, any other party or the public.

IT IS FURTHER ORDERED that, Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants are temporarily restrained and enjoined from (1) using and infringing Sophos's trademark, including specifically Sophos's registered trademark "Sophos" and/or other trademarks, trade names, service marks, or Internet Domain addresses or names containing or infringing such trademarks, trade names or service

marks; (2) using in connection with Defendants' activities, products, or services any false or deceptive designation, representation or description of Defendants or of their activities, whether by symbols, words, designs or statements, which would damage or injure Sophos or give Defendants an unfair competitive advantage or result in deception in Sophos's markets and channels of trade; or (3) acting in any other manner which suggests in any way that Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Sophos, or passing off Defendants' activities, products or services as Sophos's.

IT IS FURTHER ORDERED that, with respect to any currently registered Internet domains set forth in **Appendix A** to this Order, the domain registries set forth in Appendix A shall take the following actions:

A. Within five (5) business days of receipt of this Order, shall unlock and change the registrar of record for the domains to Lexsynergy Ltd. or such other registrar specified by Sophos. To the extent the registrar of record does not assist in changing the registrar of record for the domains under its control, the domain registry for the domains, or its administrators, including backend registry operators or administrators, within five (5) business days of receipt of this Order, shall change, or assist in changing, the registrar of record for the domains to Lexsynergy Ltd. or such other registrar specified by Sophos. The purpose of this paragraph is to ensure that Sophos has control over the hosting and administration of the domains in its registrar account at Lexsynergy Ltd. or such other registrar specified by Sophos. Sophos shall provide to the domain registry or registrar of record any requested registrar information or account details necessary to effectuate the foregoing.

B. The WHOIS registrant, administrative, billing and technical contact and identifying information should be the following, or other information as may be specified by Sophos:

Domain Administrator
Sophos Ltd.
The Pentagon, Abingdon Science Park
Abingdon OX14 3YP
United Kingdom
registrar@sophos.com

C. Prevent transfer, modification or deletion of the domain by Defendants and prevent transfer or control of the domain to the account of any party other than Sophos;

D. Take all steps required to propagate to the foregoing changes through the Domain Name System ("DNS"), including domain registrars.

IT IS FURTHER ORDERED that copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint may be served by any means authorized by law, including (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to Defendants' domain registrars and/or hosting companies and as agreed to by Defendants in the domain registration and/or hosting agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent Defendants provided accurate contact information in the U.S.; and (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Defendants, to the extent Defendants provided accurate contact information in foreign countries that are signatories to such treaties.

IT IS FURTHER ORDERED, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before this Court on May 12, 2020 at 2:00 PM by teleconference to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final

ruling on the Complaint against Defendants, enjoining Defendants from the conduct temporarily restrained by the preceding provisions of this Order.

IT IS FURTHER ORDERED that Sophos shall post bond in the amount of $10,000 to be paid into the Court registry.

IT IS FURTHER ORDERED that Sophos may identify and update the domains in **Appendix A** to this Order and the Complaint as may be reasonably necessary to account for additional Internet domains associated with Defendants' illegal conduct just prior to or within a reasonable time after the execution of this Order.

IT IS FURTHER ORDERED that Defendants shall file with the Court and serve on Sophos's counsel any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later than one (1) day prior to the hearing on Sophos's request for a preliminary injunction.

IT IS SO ORDERED

Entered this 1st day of May, 2020
2:28pm

/s/
Liam O'Grady
United States District Judge
UNITED STATES DISTRICT JUDGE

Exhibit 11

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

MICROSOFT CORPORATION, a Washington corporation, Plaintiff, v. JOHN DOES 1-2 CONTROLLING A COMPUTER NETWORK THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS, Defendants.	Civil Action No: 1:20CV730 **FILED UNDER SEAL PURSUANT TO LOCAL CIVIL RULE 5**

***EX PARTE* TEMPORARY RESTRAINING ORDER AND**
ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

Plaintiff Microsoft Corporation ("Microsoft") has filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); and (3) the common law of trespass to chattels, conversion and unjust enrichment. Microsoft has moved *ex parte* for an emergency temporary restraining order and an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C. § 1116(a) (the Lanham Act), and 28 U.S.C. § 1651(a) (the All-Writs Act).

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Microsoft's *Ex Parte* Application for an Emergency Temporary Restraining Order and Order to Show Cause re Preliminary Injunction, the Court hereby makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case, and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against Defendants John Doe 1 and 2 ("Defendants") under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Lanham Act (15 U.S.C. §§ 1114, 1125), and the common law of trespass to chattels, conversion and unjust enrichment.

2. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030) and the Lanham Act (15 U.S.C. §§ 1114, 1125), and constitute trespass to chattels, conversion and unjust enrichment, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. Microsoft owns the registered trademarks Microsoft, Microsoft corporate logo, OneDrive, SharePoint and Office 365 and numerous other trademarks used in connection with its services, software and products. There is good cause to believe that, unless Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations. The evidence set forth in Microsoft's Brief in Support of *Ex Parte* Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Application"), and the accompanying declarations and exhibits, demonstrates that Microsoft is likely to prevail on its claim that Defendants have engaged and are likely to engage in violations of the foregoing law by:

   a. intentionally accessing protected computers and sending malicious Web Apps to protected computers and computer networks of Microsoft, and to the online accounts of Microsoft's customers, without authorization or exceeding authorization, and/or attempting the activities, in order to:

      i. steal and exfiltrate information from those computers, online accounts, and computer networks;

      ii. attack and compromise the security of Microsoft's protected computers

and networks, and the online accounts of Microsoft's customers, by conducting remote reconnaissance, stealing authentication tokens and credentials, monitoring the activities of users, and using other instrumentalities of theft; and

iii. defraud Microsoft's customers.

b. deploying computers, internet domains and IP addresses by which means Defendants conduct and/or attempt to conduct illegal activities, including attacks on computers, online accounts, and networks, monitoring activities of users, theft of information stored in online accounts and defrauding Microsoft's customers;

4. There is good cause to believe that if such conduct continues, irreparable harm will occur to Microsoft, Microsoft's customers, and the public. There is good cause to believe that the Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court.

5. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of evidence of Defendants' misconduct that is hosted at and otherwise operates through the internet domains listed in Appendix A to this Order, if Defendants receive advance notice of this action. Based on the evidence cited in Microsoft's TRO Application and accompanying declarations and exhibits, Microsoft is likely to be able to prove that:

a. Defendants are engaged in activities that directly violate United States law and harm Microsoft and the public, including Microsoft's customers;

b. Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests;

c. Defendants are likely to delete or to relocate the technical infrastructure at issue in Microsoft's TRO Application and listed in Appendix A, thereby permitting them to continue their illegal acts; and

d. Defendants are likely to warn their associates engaged in such activities if informed of Microsoft's action.

6. Microsoft's request for this emergency *ex parte* relief is not the result of any lack of diligence on Microsoft's part, but instead based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), 15 U.S.C. § 1116(a) and 28 U.S.C. § 1651(a), good cause and the interest of justice require that this Order be Granted without prior notice to Defendants, and accordingly, Microsoft is relieved of the duty to provide Defendants with prior notice of Microsoft's motion.

7. There is good cause to believe that Defendants have specifically directed their activities at Microsoft's customers located in Virginia and the Eastern District of Virginia, have engaged in illegal activity using the internet domains identified in Appendix A by using those domains to deceive users of Microsoft's products and services and by directing and/or attempting to direct Web Apps software, code, commands and content to protected computers and networks of Microsoft and to the online accounts of Microsoft's customers for the purpose of perpetuating illegal conduct and causing damage to Microsoft. There is good cause to believe that Defendants have directed said Web Apps software, code, commands and content through certain instrumentalities – specifically the internet domains and the internet domain registration facilities of the domain registries identified in Appendix A.

8. There is good cause to believe that Defendants have engaged in illegal activity by using the internet domain registration facilities of the internet domain registries identified in Appendix A to register the internet domains identified in Appendix A, so as to deceive Microsoft's customers to attempt to steal authentication tokens and credentials for their Microsoft online accounts, and to deliver and/or attempt to deliver from those domains the malicious Web Apps software, code, commands and content that Defendants use to attempt to access Microsoft's services without authorization and to attempt to obtain information stolen

from those accounts and computers.

9. There is good cause to believe that Defendants have engaged in illegal activity by using deceptive and fraudulent methods to attempt to steal computer users' account authentication tokens and credentials and to attempt to use such tokens and credentials for illegal purposes, including unlawful access of online accounts.

10. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants must be prohibited from accessing Microsoft's services without authorization and prohibited from sending Web Apps software, code, commands and content from the internet domains identified in Appendix A to the protected computers and networks of Microsoft and to the online accounts of Microsoft's customers.

11. There is good cause to believe that Defendants have engaged in illegal activity using the internet domains identified in Appendix A to attempt to compromise accounts of Microsoft's customers and to attempt to steal information from them. There is good cause to believe that to immediately halt the injury caused by Defendants, each of Defendants' domains set forth in Appendix A must be immediately transferred beyond the control of Defendants, thus making them inaccessible to Defendants.

12. There is good cause to believe that to immediately halt the injury, the execution of this Order should be carried out in a coordinated manner by Microsoft and by the domain registries and the internet hosting companies identified in Appendix A on such date and time within five (5) days of this Order as may be reasonably requested by Microsoft.

13. There is good cause to permit notice of the instant Order, notice of the Preliminary Injunction hearing and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of

service are authorized by law, satisfy Due Process, and satisfy Fed. R. Civ. P. 4(f)(3) and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to Defendants' domain registrars and hosting companies and as agreed to by Defendants in Defendants' domain registration and/or hosting agreements, (2) publishing notice on a publicly available internet website, (3) by personal delivery upon Defendants, to the extent Defendants provided accurate contact information in the U.S.; and (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Defendants, to the extent Defendants provided accurate contact information in foreign countries that are signatories to such treaties.

TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

IT IS THEREFORE ORDERED that, Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants, are temporarily restrained and enjoined from: (1) intentionally accessing protected computers and sending malicious Web Apps software, code, commands and content to the protected computers and computer networks of Microsoft and to the online accounts of customers of Microsoft, without authorization or exceeding authorization; (2) stealing and exfiltrating information from the foregoing computers, computer networks and online accounts; (3) attacking and compromising the security of the foregoing computers, computer networks and online accounts by conducting remote reconnaissance, stealing authentication tokens and credentials, monitoring the activities of users, and using other instrumentalities of theft; (4) defrauding Microsoft's customers, (5) deploying computers, internet domains and IP addresses to conduct illegal activities, including attacks on computers and networks, monitoring activities of users, and theft of information stored in online

accounts; (6) using deceptive and fraudulent methods to attempt to steal computer users' authentication tokens and online account credentials and to attempt to use such tokens and credentials for illegal purposes; (6) accessing Microsoft's services without authorization and sending malicious Web Apps software, code, commands and content from the internet domains identified in Appendix A to the computers and computer networks of Microsoft and to the online accounts of Microsoft's customers; (7) using the internet domains identified in Appendix A to attempt to compromise accounts of Microsoft's customers and to attempt to steal information from them; (8) configuring, deploying, operating, or otherwise participating in or facilitating infrastructure described in the TRO Application, including but not limited to the software operating through the internet domains set forth in Appendix A and through any other component or element of the Defendants' illegal infrastructure at any location; (9) stealing information from Microsoft's customers; (10) misappropriating that which rightfully belongs to Microsoft, its customers, or in which Microsoft or its customers have a proprietary interest; or (11) undertaking any similar activity that inflicts harm on Microsoft, Microsoft's customers, or the public.

IT IS FURTHER ORDERED that, Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants are temporarily restrained and enjoined from (1) using and infringing Microsoft's trademarks, including specifically Microsoft's registered trademarks Microsoft, Microsoft corporate logo, OneDrive, SharePoint and Office 365 and/or other trademarks, trade names, and/or service marks; (2) using in connection with Defendants' activities, products, or services any false or deceptive designation, representation or description of Defendants or of their activities, whether by symbols, words, designs or statements, which would damage or injure Microsoft or give Defendants an unfair

competitive advantage or result in deception of consumers; or (3) acting in any other manner which suggests in any way that Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Microsoft, or passing off Defendants' activities, products or services as Microsoft's.

IT IS FURTHER ORDERED that, with respect to any currently registered internet domains set forth in Appendix A to this Order, the domain registries located in the United States shall take the following actions:

A. Within five (5) business days of receipt of this Order, shall unlock and change the registrar of record for the domain to MarkMonitor or such other registrar specified by Microsoft. To the extent the registrar of record does not assist in changing the registrar of record for the domain under its control, the domain registry for the domain, or its administrators, including backend registry operators or administrators, within five (5) business days of receipt of this Order, shall change, or assist in changing, the registrar of record for the domain to MarkMonitor or such other registrar specified by Microsoft. The purpose of this paragraph is to ensure that Microsoft has control over the hosting and administration of the domain in its registrar account at MarkMonitor or such other registrar specified by Microsoft. Microsoft shall provide to the domain registry or registrar of record any requested registrar information or account details necessary to effectuate the foregoing.

B. The WHOIS registrant, administrative, billing and technical contact and identifying information should be the following, or other information as may be specified by Microsoft:

Domain Administrator
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

United States
Phone: +1.4258828080
Facsimile: +1.4259367329
domains@microsoft.com

C. Prevent transfer, modification or deletion of the domain by Defendants and prevent transfer or control of the domain to the account of any party other than Microsoft;

D. Take all steps required to propagate to the foregoing changes through the Domain Name System ("DNS"), including domain registrars.

E. With regard to any domain registries or registrars located outside of the United States, the Court respectfully requests, but does not order, that they take the same or substantially similar actions as the foregoing so as to neutralize the threat posed by the Defendants to the citizens of all countries, including their own. Defendants, their representatives and persons who are in active concert or participation with them are ordered to consent to whatever actions are necessary for non-United States registries, registrars and registrants or hosts, set forth in Appendix A, to effectuate this request.

IT IS FURTHER ORDERED that, with respect to the internet domains set forth in Appendix A, the domain registrars located in the United States shall preserve, retain and produce to Microsoft all documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or controlling the internet domains set forth in Appendix A, including any and all individual or entity names, mailing addresses, e-mail addresses, facsimile numbers and telephone numbers or similar contact information, including but not limited to such contact information reflected in billing, usage, access and contact records and all records, documents and logs associated with Defendants' or Defendants' representatives' use of or access to the internet domains.

IT IS FURTHER ORDERED that copies of this Order, notice of the Preliminary

Injunction hearing and service of the Complaint may be served by any means authorized by law, including (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to Defendants' internet domain registrars and/or hosting companies and as agreed to by Defendants in the internet domain registration and/or hosting agreements, (2) publishing notice on a publicly available internet website, (3) by personal delivery upon Defendants, to the extent Defendants provided accurate contact information in the U.S.; and (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Defendants, to the extent Defendants provided accurate contact information in foreign countries that are signatories to such treaties.

IT IS FURTHER ORDERED, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before this Court on July 10, 2020 at 10:00 am by telephone to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against Defendants, enjoining Defendants from the conduct temporarily restrained by the preceding provisions of this Order.

IT IS FURTHER ORDERED that Microsoft shall post a surety bond in the amount of $50,000 to be paid into the Court registry.

IT IS FURTHER ORDERED that Defendants shall file with the Court and serve on Microsoft's counsel any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later than one (1) day prior to the hearing on Microsoft's request for a preliminary injunction.

IT IS SO ORDERED

Entered this 1st day of ~~June~~ July, 2020

/s/
Liam O'Grady
United States District Judge

UNITED STATES DISTRICT JUDGE

EXHIBIT 12

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

DXC TECHNOLOGY COMPANY, a Nevada corporation, Plaintiff, v. JOHN DOES 1-2, Defendants.	Civil Action No: 1:20-cv-00814-RDA-MSN *SEALED* **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5**

[PROPOSED] *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

Plaintiff DXC Technology Company has filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) Electronic Communications Privacy Act, 18 U.S.C. § 2701(a); and (3) the common law of trespass to chattels, conversion, and unjust enrichment. DXC has moved *ex parte* for an emergency temporary restraining order and an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure and 28 U.S.C. § 1651(a) (the All Writs Act).

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of DXC's *Ex Parte* Application for an Emergency Temporary Restraining Order and Order to Show Cause re Preliminary Injunction, the Court hereby makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case, and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against Defendants John Doe 1 and 2 ("Defendants") under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Electronic Communications Privacy Act (18 U.S.C. § 2701), and common law of trespass to chattels, conversion, and unjust enrichment.

2. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Electronic Communications Privacy Act (18 U.S.C. § 2701), and constitute common law of trespass to chattels, conversion, and unjust enrichment, and that DXC is, therefore, likely to prevail on the merits of this action.

3. DXC has been the target of directed malicious acts intended to disrupt DXC's services, infiltrate DXC systems, and infect DXC's and its customers' systems with malicious ransomware software and exfiltrate information, including credentials. There is good cause to believe that, unless Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations. The evidence set forth in DXC's Brief in Support of *Ex Parte* Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Application"), and the accompanying declarations and exhibits, demonstrates that DXC is likely to prevail on its claim that Defendants have engaged in violations of the foregoing law by:

   a. intentionally accessing and sending malicious software, code, and instructions to the protected computers and operating systems of DXC, without authorization or exceeding authorization, in order to

      i. infect those computers and operating systems with malicious code and thereby attempt to gain control over those computers and operating systems;

      ii. attack the security of those computers by conducting remote

reconnaissance, and attempting to access information on those computers, without authorization;

4. There is good cause to believe that if such conduct continues, irreparable harm will occur to DXC. There is good cause to believe that the Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court.

5. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of command and control software that is hosted at and otherwise operates through the Internet domains listed in **Appendix A** to this Order and from the destruction or concealment of other discoverable evidence of Defendants' misconduct available via those domains, including on user computers infected by Defendants, if Defendants receive advance notice of this action. Based on the evidence cited in DXC's TRO Application and accompanying declarations and exhibits, DXC is likely to be able to prove that:

b. Defendants are engaged in activities that directly violate United States law and harm DXC;

c. Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests;

d. Defendants are likely to delete or to relocate the command and control software at issue in DXC's TRO Application and the harmful and malicious software disseminated through the Internet domains listed in **Appendix A** to this Order, thereby permitting them to continue their illegal acts; and

e. Defendants are likely to warn their associates engaged in such activities if informed of DXC's action.

6. DXC's request for this emergency *ex parte* relief is not the result of any lack of diligence on DXC's part, but instead based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b) and 28 U.S.C. § 1651(a), good cause and the interest of justice require that this Order be Granted without prior notice to Defendants, and

accordingly, DXC is relieved of the duty to provide Defendants with prior notice of DXC's motion.

7. There is good cause to believe that Defendants have specifically directed their activities to DXC's computers and networks devices located in Virginia, including in the vicinity of Alexandria, Virginia, and the Eastern District of Virginia, have engaged in illegal activity using the Internet domains identified in **Appendix A** to this Order by using those domains to direct malicious code to DXC's computers and networks devices to further perpetrate their illegal conduct. There is good cause to believe that Defendants have directed said malicious code and content through certain instrumentalities—specifically the domains and the domain registration facilities of the domain registries identified in **Appendix A** to this Order.

8. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants must be prohibited from accessing DXC's computers and networks devices without authorization and prohibited from sending malicious code, content and commands from the Internet domains identified in **Appendix A** to this Order to DXC's computers and networks devices.

9. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains identified in Appendix A to this Order to host the command and control software used to deliver malicious software to DXC's computers and networks devices. There is good cause to believe that to immediately halt the injury caused by Defendants, each of Defendants' current and prospective domains set forth in **Appendix A** to this Order must be immediately transferred to the control of DXC, thus making them inaccessible to Defendants for command and control purposes.

10. There is good cause to believe that to immediately halt the injury, the execution of

this Order should be carried out in a coordinated manner by DXC and by the domain registries identified in **Appendix A** to this Order on such date and time within five (5) days of this Order as may be reasonably requested by DXC.

11. There is good cause to believe that Defendants may change the Internet domains that they use to conduct illegal activities, and that DXC may identify and update the domains listed in **Appendix A** to this Order as may be reasonably necessary to account for additional Internet domains associated with Defendants just prior to the execution of this Order and within a reasonable time thereafter should Defendants attempt to evade and defy this Order.

12. There is good cause to permit notice of the instant Order, notice of the Preliminary Injunction hearing and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, and satisfy Fed. R. Civ. P. 4(f)(3) and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to Defendants' domain registrar and registries and hosting companies and as agreed to by Defendants in Defendants' domain registration and/or hosting agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent Defendants provided accurate contact information in the U.S.; and/or (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Defendants, to the extent Defendants provided accurate contact information in foreign countries that are signatories to such treaties.

TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

IT IS THEREFORE ORDERED that, Defendants, Defendants' representatives, and

persons who are in active concert or participation with Defendants, are temporarily restrained and enjoined from: (1) intentionally accessing and sending malicious software or code to DXC's protected computers, including its computers and networks devices, or the computers or networks of any other party, without authorization; (2) intentionally attacking and compromising computers or networks of DXC or the computers or networks of any other party, to access computing resources and information on those devices, or for any other illegal purpose; (3) configuring, deploying, operating, or otherwise participating in or facilitating a command and control infrastructure described in the TRO Application, including but not limited to the command and control software hosted at and operating through the Internet domains set forth in **Appendix A** to this Order and through any other component or element of the command and control infrastructure at any location; (4) stealing or exfiltrating information from DXC or any other party, including through the foregoing activities; (5) delivering malicious software designed to steal account credentials, (6) delivering malicious "ransomware" software designed to lock access to computers and demand a ransom from victims, (7) carrying out fraudulent schemes, (8) misappropriating that which rightfully belongs to DXC or any other party, or in which DXC or any other party has a proprietary interest, including through the foregoing activities; (9) downloading or offering to download additional malicious software onto DXC's computers and networks or the computer of any other party; (10) monitoring the activities of DXC's customers and stealing information from them, (11) attacking computers and networks, monitoring activities of users, and theft of information or (12) undertaking any similar activity that inflicts harm on DXC, any other party or the public.

IT IS FURTHER ORDERED that, with respect to any currently registered Internet domains set forth in **Appendix A** to this Order, the domain registrar and registries set forth in

Appendix A shall take the following actions:

A. Within two (2) business days of receipt of this Order, and as soon as is possible, shall unlock and change the registrar of record for the domains to MarkMonitor or such other registrar specified by DXC. To the extent the registrar of record does not assist in changing the registrar of record for the domains under its control, the domain registry for the domains, or its subsidiaries, within two (2) business days of receipt of this Order, shall change, or assist in changing, the registrar of record for the domains MarkMonitor or such other registrar specified by DXC. The purpose of this paragraph is to ensure that DXC has control over the hosting and administration of the domains in its registrar account at MarkMonitor or such other registrar specified by DXC. DXC shall provide to the domain registry or registrar of record any requested registrar information or account details necessary to effectuate the foregoing.

B. The WHOIS registrant, administrative, billing and technical contact and identifying information should be the following, or other information as may be specified by DXC:

Domain Administrator
DXC Technology Company
1775 Tysons Blvd
Tysons, Virginia 22102
United States
Webmaster@dxc.com

C. Prevent transfer, modification or deletion of the domain by Defendants and prevent transfer or control of the domain to the account of any party other than DXC;

D. Take all steps required to propagate to the foregoing changes through the Domain Name System ("DNS"), including domain registrar and registries.

IT IS FURTHER ORDERED that copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint may be served by any means

authorized by law, including (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to Defendants' domain registrar and registries and/or hosting companies and as agreed to by Defendants in the domain registration and/or hosting agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent Defendants provided accurate contact information in the U.S.; and (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Defendants, to the extent Defendants provided accurate contact information in foreign countries that are signatories to such treaties.

IT IS FURTHER ORDERED, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before this Court on **August 5, 2020 at 11:00 A.M.** to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against Defendants, enjoining Defendants from the conduct temporarily restrained by the preceding provisions of this Order.

IT IS FURTHER ORDERED that DXC shall post bond in the amount of $ 50,000 to be paid into the Court registry.

IT IS FURTHER ORDERED that DXC may identify and update the domains in **Appendix A** to this Order and the Complaint as may be reasonably necessary to account for additional Internet domains associated with Defendants' illegal conduct just prior to or within a reasonable time after the execution of this Order.

It is FURTHER ORDERED that Defendants shall file with the Court and serve on DXC's counsel any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later the Friday prior to the hearing on DXC's request for preliminary injunction.

It is SO ORDERED.

Alexandria, Virginia
July 22, 2020 at 1:20 p.m.

/s/
Rossie D. Alston, Jr.
United States District Judge

EXHIBIT 13

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

MICROSOFT CORPORATION, a Washington corporation, and FS-ISAC, INC., a Delaware corporation, Plaintiffs, v. JOHN DOES 1-2, CONTROLLING A COMPUTER BOTNET AND THEREBY INJURING PLAINTIFFS, AND THEIR CUSTOMERS AND MEMBERS, Defendants.	Civil Action No: 1:20cv1171 **FILED UNDER SEAL**

***EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

Plaintiffs Microsoft Corp. ("Microsoft") and Financial Services – Information Sharing And Analysis Center, Inc. ("FS-ISAC") (collectively "Plaintiffs") have filed a complaint for injunctive and other relief pursuant to: (1) the Copyright Act (17 U.S.C. § 101, *et seq.*); (2) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (3) the Electronic Communications Privacy Act (18 U.S.C. § 2701); (4) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); and (5) the common law of trespass, unjust enrichment and conversion. Plaintiffs have moved *ex parte* for an emergency temporary restraining order and an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C. § 1116(a) (the Lanham Act), and 28 U.S.C. § 1651(a) (the All-Writs Act).

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Plaintiffs' Application for an Emergency Temporary Restraining Order, the Court hereby makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case and there is good

cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against Defendants John Does 1-2 ("Defendants") under the Copyright Act (17 U.S.C. §§ 106 and 501 *et seq.*), the Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125) and the common law of trespass to chattels, unjust enrichment and conversion.

2. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Copyright Act (17 U.S.C. §§ 106 and 501 *et seq.*), the Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125) and constitute trespass to chattels, unjust enrichment and conversion, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. Microsoft owns the registered copyrights in the Windows 8 Software Development Kit ("SDK"), Reg. No. TX 8-888-365 ("Copyrighted Work"). Microsoft's Copyrighted Work is an original, creative work and copyrightable subject matter under the laws of the United States. *See* 17 U.S.C. § 102(a); *see also Oracle America, Inc. v. Google Inc.*, 750 F.3d 1339 (Fed. Cir. 2014) (holding the structure, sequence, and organization of declaring computer code qualifies as an original work under the Copyright Act).

4. Microsoft owns the registered trademarks "Microsoft" and "Windows" used in connection with its services, software and products. FS-ISAC's member organizations have invested in developing their brands, trademarks, and trade names in association with the financial services they offer.

5. There is good cause to believe that, unless Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations. The evidence set forth in Plaintiffs' Brief in Support of Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Application"),

and the accompanying declarations and exhibits, demonstrates that Plaintiffs are likely to prevail on their claims that Defendants have engaged in violations of the foregoing law by:

a. directly, contributorily and through inducement, infringing Microsoft's Copyrighted Work by reproducing, distributing, and creating derivative works in their malicious software, which includes code that is literally copied from, substantially similar to and derived from the Copyrighted Work, in violation of Microsoft's exclusive rights at least under 17 U.S.C. § 101 *et seq.* without any authorization or other permission from Microsoft;

b. transmitting malicious code containing the Copyrighted Work through Internet Protocol addresses ("IP Addresses") to configure, deploy and operate a botnet;

c. intentionally accessing and sending malicious software, code, and instructions to the protected computers and operating systems of the customers or associated member organizations of Microsoft and FS-ISAC, without authorization and exceeding authorization, in order to

   i. install on those computers and computer networks malicious code and thereby gain control over those computers and computer networks in order to make them part of the computer botnet known as the "Trickbot" botnet (the "botnet");

   ii. attack and compromise the security of those computers and computer networks by conducting remote reconnaissance, stealing and harvesting authentication credentials, monitoring the activities of users, and using other instrumentalities of theft;

   iii. steal and exfiltrate information from those computers and computer networks;

d. corrupting Microsoft's operating system and applications on victims' computers and networks, thereby using them to carry out the foregoing activities

e. creating false websites that falsely indicate that they are associated with or approved by Plaintiffs or Plaintiffs' member organizations;

f. stealing personal and financial account information from computer users; and

g. using stolen information to steal money from the financial accounts of those users.

6. There is good cause to believe that if such conduct continues, irreparable harm will occur to Plaintiffs, Plaintiffs' customers and member organizations, and the public. There is good cause to believe that the Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court;

7. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of botnet command and control software that is hosted at and otherwise operates through the IP addresses listed in **Appendix A** and from the destruction or concealment of other discoverable evidence of Defendants' misconduct available at those locations if Defendants receive advance notice of this action. Based on the evidence cited in Plaintiffs' TRO Application and accompanying declarations and exhibits, Plaintiffs are likely to be able to prove that:

a. Defendants are engaged in activities that directly violate United States law and harm Plaintiffs and the public, including Plaintiffs' customers and member-organizations;

b. Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests;

c. Defendants are likely to delete or to relocate the botnet command and control software at issue in Plaintiffs' TRO Application and the harmful and malicious software, infringing Microsoft's Copyrighted Work and trademarks, disseminated through the IP Addresses listed in **Appendix A** to this Order, thereby permitting them to continue their illegal acts; and

d. Defendants are likely to warn their associates engaged in such activities if informed of Plaintiffs' action.

8. Plaintiffs' request for this emergency *ex parte* relief is not the result of any lack of diligence on Plaintiffs' part, but instead based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), 15 U.S.C. § 1116(a) and 28 U.S.C. § 1651(a), good cause and the interest of justice require that this Order be Granted without prior notice to Defendants, and accordingly, Plaintiffs are relieved of the duty to provide Defendants with prior notice of Plaintiffs' motion.

9. There is good cause to believe that Defendants have specifically directed their activities to computers of Plaintiffs' customers and member organizations located in the Eastern District of Virginia, have engaged in illegal activity using the IP Addresses identified in **Appendix A** to this Order that are registered to command and control servers located at data

centers and/or hosting companies set forth in **Appendix A**, to direct malicious botnet code and content through the Internet to said computers of Plaintiffs' customers and member organizations to further perpetrate their fraud on Plaintiffs' customers and member organizations.

10. There is good cause to believe that Defendants have engaged in illegal activity using the data centers and/or Internet hosting providers identified in **Appendix A** to host command and control software and the malicious botnet code and content used to maintain and operate the botnet at computers, servers, electronic data storage devices, or media at the IP Addresses listed in **Appendix A**.

11. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants' IP Addresses identified in **Appendix A** must be immediately disabled; Defendants' computer resources related to such IP Addresses must be disconnected from the Internet; Defendants must be prohibited from accessing Defendants' computer resources related to such IP Addresses; and to prevent the destruction of data and evidence located on those computing resources.

12. There is good cause to believe that in order to immediately halt the injury caused by Defendants and to ensure the future prosecution of this case it not rendered fruitless by attempts to delete, hide, conceal, or otherwise render inaccessible the software components that create, distribute, and are involved in the creation, perpetuation, and maintenance of the botnet and prevent the unauthorized copying, reproduction, distribution, public display, and creation of derivative works in Microsoft's Copyrighted Work and prevent the creation and distribution of unauthorized copies of the registered trademarks of Microsoft and FS-ISAC's member organizations and carry out other harmful conduct, with respect to the Defendants' most current, active command and control servers hosted at the IP Addresses, the following actions should be taken. The data centers and/or hosting companies set forth in **Appendix A** should take reasonable steps to block incoming and/or outgoing traffic on their respective networks that originates or has been sent from and/or to the IP Addresses identified in **Appendix A**, such that

said traffic will not reach victim end-user computers on the ISPs' respective networks and/or the computers at the IP Addresses in **Appendix A**, and should take other reasonable steps to block such traffic to and/or from any other IP addresses to which Defendants may move the botnet infrastructure, identified by Plaintiffs and which the Court may order to be subject to this Order, to ensure that Defendants cannot use such infrastructure to control the botnet.

13. There is good cause to believe that Defendants may change the IP Addresses that they use to conduct illegal activities, and that Plaintiffs may identify and update the IP Addresses listed in **Appendix A** to this Order as may be reasonably necessary to account for additional IP Addresses associated with Defendants just prior to the execution of this Order and within a reasonable time thereafter should Defendants attempt to evade and defy this Order.

14. There is good cause to permit notice of the instant Order, notice of the Preliminary Injunction hearing and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, and satisfy Fed. R. Civ. P. 4(f)(3) and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to Defendants' data centers and/or hosting companies and as agreed to by Defendants in Defendants' data center and/or hosting agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent Defendants provided accurate contact information in the U.S.; and (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Defendants, to the extent Defendants provided accurate contact information in foreign countries that are signatories to such treaties.

15. There is good cause to believe that the harm to Microsoft and FS-ISAC's member organizations of denying the relief requested in the TRO Application outweighs any harm to any legitimate interests of Defendants and that there is no undue burden to any third party.

TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

IT IS THEREFORE ORDERED that, Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from: (1) intentionally accessing and sending malicious software or code to Plaintiffs and the protected computers and operating systems of Plaintiffs' customers and associated member organizations, without authorization, in order to infect those computers and make them part of any botnet, (2) sending malicious code to configure, deploy and operate a botnet, (3) attacking and compromising the security of the computers and networks of Plaintiffs, their customers, and any associated member organizations, (4) stealing and exfiltrating information from computers and computer networks, (5) creating false websites that falsely indicated that they are associated with or approved by Plaintiffs or Plaintiffs' member organizations; (6) configuring, deploying, operating, or otherwise participating in or facilitating the botnet described in the TRO Application, including but not limited to the command and control software hosted at and operating through the IP Addresses set forth herein and through any other component or element of the botnet in any location; (7) delivering malicious software designed to steal financial account credentials, (8) monitoring the activities of Plaintiffs, Plaintiffs' customers or member associations and stealing information from them, (9) attacking computers and networks, monitoring activities of users, and theft of information, (10) corrupting Microsoft's operating system and applications on victims' computers and networks, thereby using them to carry out the foregoing activities, (11) misappropriating that which rightfully belongs to Plaintiffs, Plaintiffs' customers or member associations or in which Plaintiffs have a proprietary interests, and (12) undertaking any similar activity that inflicts harm on Plaintiffs, Plaintiffs' customers or member associations, or the public.

IT IS FURTHER ORDERED that, Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from: (1) reproducing, distributing, creating derivative works, and/or otherwise infringing Microsoft's

Copyrighted Work, bearing registration number TX 8-888-365; (2) using and infringing Microsoft's trademarks, including specifically Microsoft's registered trademarks "Microsoft," "Windows," "Outlook" and "Word" logo bearing registration numbers 2872708, 5449084, 2463526, 4255129 and 77886830; and/or the trademarks of financial institution members of FS-ISAC; (2) using in connection with Defendants' activities, products or services any false or deceptive designation, representation or description of Defendants or of their activities, whether by symbols, words, designs or statements, which would damage or injure Plaintiffs or their member organizations or give Defendants an unfair competitive advantage or result in deception of consumers; or (3) acting in any other manner which suggests in any way that Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Microsoft, or passing off Defendants' activities, products or services as Plaintiffs' or their member organizations.

IT IS FURTHER ORDERED that, with respect to any of the IP Addresses set forth in **Appendix A** to this Order, the data centers and/or hosting providers identified in **Appendix A** to this Order shall take reasonable best efforts to implement the following actions:

A. Take reasonable steps to identify incoming and/or outgoing Internet traffic on their respective networks that originates and/or is being sent from and/or to the IP Addresses identified in **Appendix A**;

B. Take reasonable steps to block incoming and/or outgoing Internet traffic on their respective networks that originate and/or are being sent from and/or to the IP Addresses identified in **Appendix A**, by Defendants or Defendants' representatives or resellers, except as explicitly provided for in this Order;

C. Take other reasonable steps to block such traffic to and/or from any other IP addresses or domains to which Defendants may move the botnet infrastructure, identified by Microsoft in a supplemental request to this Order, to ensure that Defendants cannot use such infrastructure to control the botnet.

D. Completely disable the computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with the IP Addresses set forth in **Appendix A** and make them inaccessible from any other computer on the Internet, any internal network, or in any other manner, to Defendants, Defendants' representatives and all other persons, except as otherwise ordered herein;

E. Completely, and until further order of this Court, suspend all services to Defendants or Defendants' representatives or resellers associated with the IP Addresses set forth in **Appendix A**;

F. Transfer any content and software hosted at the IP Addresses listed in **Appendix A** that are not associated with Defendants, if any, to new IP Addresses not listed in **Appendix A**; notify any non-party owners of such action and the new IP addresses, and direct them to contact Microsoft's counsel, Gabriel M. Ramsey, Crowell & Moring LLP, 3 Embarcadero Ctr., 26th Floor, San Francisco, CA 94111, gramsey@crowell.com, (Tel: 415-365-7207), to facilitate any follow-on action;

G. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from publicizing this Order until this Order is executed in full, except as necessary to communicate with hosting companies, data centers, the Plaintiffs or other ISPs to execute this order;

H. Not enable, and shall take all reasonable steps to prevent, any circumvention of this order by Defendants or Defendants' representatives associated with the IP Addresses, including without limited to enabling, facilitating, and/or allowing Defendants or Defendants' representatives or resellers to rent, lease, purchase, or otherwise obtain another IP Address associated with your services;

I. Preserve, retain and produce to Plaintiffs all documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or controlling the IP Addresses set forth in **Appendix A**, including any and all individual or entity names, mailing

addresses, e-mail addresses, facsimile numbers and telephone numbers or similar contact information, including but not limited to such contact information reflected in billing, usage, access and contact records and all records, documents and logs associated with Defendants' or Defendants' Representatives' use of or access to the IP Addresses;

J. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order; and

K. Completely preserve the computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with the IP Addresses set forth in **Appendix A**, and preserve all evidence of any kind related to the content, data, software or accounts associated with such IP addresses and such computer hardware, such that such evidence of Defendants' unlawful activities is preserved.

IT IS FURTHER ORDERED that copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint may be served by any means authorized by law, including any one or combination of (1) personal delivery upon Defendants who provided accurate contact information in the U.S., if any; (2) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided accurate contact information in foreign countries that are signatory to such treaties, if any, (3) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their hosting companies and as agreed to by Defendants in their hosting agreements, (4) publishing notice on a publicly available Internet website and/or in newspapers in the communities where Defendants are believed to reside.

IT IS FURTHER ORDERED, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before this Court on October 20th, 2020, at 2:00 p.m. to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against the Defendants, enjoining them from the conduct temporarily restrained by the preceding provisions of this Order.

IT IS FURTHER ORDERED that Microsoft shall post bond in the amount of $75,000 as cash to be paid into the Court registry.

IT IS FURTHER ORDERED that Plaintiffs may identify and update the IP addresses to this Order as may be reasonably necessary to account for additional IP addresses associated with the Trickbot Botnet just prior to the execution of this Order.

IT IS FURTHER ORDERED that the Defendants shall file with the Court and serve on Plaintiffs' counsel any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later than two (2) days prior to the hearing on Microsoft's request for a preliminary injunction. Plaintiffs may file responsive or supplemental pleadings, materials, affidavits, or memoranda with the Court and serve the same on counsel for the Defendants no later than one (1) day prior to the preliminary injunction hearing in this matter. Provided that service shall be performed by personal or overnight delivery, facsimile or electronic mail, and documents shall be delivered so that they shall be received by the other parties no later than 4:00 p.m. (Eastern Standard Time) on the appropriate dates listed in this paragraph.

IT IS SO ORDERED

Entered this 6th day of October, 2020.

/s/
Anthony J. Trenga
United States District Judge

Exhibit 14

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

MICROSOFT CORPORATION, a Washington corporation, FS-ISAC, INC., a Delaware corporation and HEALTH-ISAC, INC., a Florida corporation, Plaintiffs, v. DENIS MALIKOV AND JOHN DOES 1-7, Defendants.	Case No.: 1:22-CV-1328-MHC **FILED UNDER SEAL**

EX PARTE TEMPORARY RESTRAINING ORDER AND
ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

Plaintiffs Microsoft Corp. ("Microsoft"), FS-ISAC, Inc. ("FS-ISAC") and HEALTH-ISAC, Inc. ("H-ISAC") have filed a complaint for injunctive and other relief pursuant to, *inter alia*: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) the Electronic Communications Privacy Act (18 U.S.C. § 2701); (3) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); (7) the Georgia Computer Systems Protection Act (O.C.G.A. § 16-9-93) and (4) the common law of trespass

to chattels, unjust enrichment and conversion. Plaintiffs have moved *ex parte* for an emergency temporary restraining order and an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C. § 1116(a) (the Lanham Act), and 28 U.S.C. § 1651(a) (the All-Writs Act).

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Plaintiffs' Application for an Emergency Temporary Restraining Order, the Court hereby makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case, and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against Defendants Denis Malikov and John Does 1 through 7 ("Defendants") under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)), the Georgia Computer Systems Protection Act (O.C.G.A. § 16-9-93) and the common law of trespass to chattels, unjust enrichment and conversion.

2. There is good cause to believe that Defendants have engaged in and

are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)), the Georgia Computer Systems Protection Act (O.C.G.A. § 16-9-93) and the common law of trespass to chattels, unjust enrichment and conversion, and that Microsoft is, therefore, likely to prevail on the merits of this action.

3. Microsoft owns the registered trademarks "Microsoft," "Windows," "Excel" and "Word," used in connection with its services, software and products. FS-ISAC's members own registered trademarks in their names and logos used in connection with their online financial services.

4. There is good cause to believe that, unless Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations. The evidence set forth in Plaintiffs' Brief in Support of Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Application"), and the accompanying declarations and exhibits, demonstrates that Plaintiffs are likely to prevail on their claim that Defendants have engaged in violations of the foregoing law by:

a. intentionally accessing and sending malicious software, code, and instructions to the protected computers, operating systems, and

computer networks of Microsoft, the customers of Microsoft and the members of FS-ISAC and H-ISAC, without authorization or exceeding authorization, in order to

i. infect those computers and computer networks with malicious code and thereby gain control over those computers and computer networks;

ii. attack and compromise the security of those computers and computer networks by conducting remote reconnaissance, stealing authentication credentials, monitoring the activities of users, and using other instrumentalities of theft;

iii. steal and exfiltrate information from those computers and computer networks;

b. deploying computers and Internet domains to establish a command and control infrastructure by which means Defendants conduct illegal activities, including attacks on computers and networks, monitoring activities of users, and theft of information;

c. corrupting Microsoft's operating system and applications on victims' computers and networks, thereby using them to monitor the activities of users and steal information from them;

5. There is good cause to believe that if such conduct continues, irreparable harm will occur to Microsoft, Microsoft's customers, FS-ISAC's and H-ISAC's members and the public. There is good cause to believe that the Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court.

6. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale,

transfer, or other disposition or concealment by Defendants of command and control software that is hosted at and otherwise operates through the Internet domains listed in **Appendix A** to this Order and from the destruction or concealment of other discoverable evidence of Defendants' misconduct available via those domains, including on user computers infected by Defendants, if Defendants receive advance notice of this action. Based on the evidence cited in Plaintiffs' TRO Application and accompanying declarations and exhibits, Plaintiffs are likely to be able to prove that:

a. Defendants are engaged in activities that directly violate United States law and harm Microsoft, Microsoft's customers, FS-ISAC's and H-ISAC's members and the public;

b. Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests;

c. Defendants are likely to delete or to relocate the command and control software at issue in Plaintiffs' TRO Application and the harmful and malicious software disseminated through the Internet domains listed in Appendix A, thereby permitting them to continue their illegal acts; and

7. Plaintiffs' request for this emergency *ex parte* relief is not the result of any lack of diligence on Plaintiffs' part, but instead based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), 15 U.S.C. § 1116(a) and 28 U.S.C. § 1651(a), good cause and the interest of justice require that this Order be Granted without prior notice to Defendants, and

accordingly, Plaintiffs are relieved of the duty to provide Defendants with prior notice of Microsoft's motion.

8. There is good cause to believe that Defendants have specifically directed their activities to computers of Plaintiffs customers and members located in the Northern District of Georgia, have engaged in illegal activity using the Internet domains identified in **Appendix A** to this Order by directing malicious code and content to said computers of Plaintiffs' customers and members to further perpetrate their illegal conduct victimizing those parties. There is good cause to believe that Defendants have directed said malicious code and content through certain instrumentalities – specifically the domains and the domain registration facilities of the domain registries identified in **Appendix A**.

9. There is good cause to believe that Defendants have engaged in illegal activity by using the domain registration facilities of the domain registries identified in **Appendix A** to register the Internet domains identified in **Appendix A**, so as to deliver from those domains the malicious code, content, and commands that Defendants use to access Plaintiffs' and their customers' and members' computers, networks and services without authorization and to infect and compromise the computers of Microsoft's customers and FS-ISAC's and H-ISAC's members, and to receive the information stolen from those computers.

10. There is good cause to believe that Defendants have engaged in illegal activity by using deceptive and fake methods to steal computer users' login and/or account credentials and to use such credentials for illegal purposes.

11. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants must be prohibited from accessing Plaintiffs' and their customers' and members' computers, networks and services without authorization and be prohibited from sending malicious code, content and commands from the Internet domains identified in **Appendix A** to the computers of Plaintiffs, their customers and their members.

12. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains identified in **Appendix A** to host the command and control software and content used to infect and compromise the computers and networks of Plaintiffs and their customers and members and to steal information from them. There is good cause to believe that to immediately halt the injury caused by Defendants, each of Defendants' current and prospective domains set forth in **Appendix A** must be immediately redirected to the Plaintiff-secured name-servers ns081a.microsoftinternetsafety.net and ns081b.microsoftinternetsafety.net, thus making them inaccessible to Defendants for command and control purposes.

13. There is good cause to believe that to immediately halt the injury, the execution of this Order should be carried out in a coordinated manner by Plaintiffs and by the domain registries identified in **Appendix A** on such date and time within five (5) business days of this Order as may be reasonably requested by Plaintiffs.

14. There is good cause to permit notice of the instant Order, notice of the Preliminary Injunction hearing and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, and satisfy Fed. R. Civ. P. 4(f)(3) and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to Defendants' domain registrars and hosting companies and as agreed to by Defendants in Defendants' domain registration and/or hosting agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent Defendants provided accurate contact information in the U.S.; and/or (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Defendants, to the extent Defendants provided accurate contact information in

foreign countries that are signatories to such treaties.

TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

IT IS THEREFORE ORDERED that, Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants, are temporarily restrained and enjoined from: (1) intentionally accessing and sending malicious software or code to Plaintiffs, their customers and members, and the protected computers and operating systems of Microsoft, Microsoft's customers, and FS-ISAC's and H-ISAC's members without authorization, in order to infect those computers; (2) intentionally attacking and compromising computers or computer networks of Plaintiffs, their customers and members, to monitor the activities of the owners or users of those computers or computer networks, and to steal information from those computers or networks; (3) configuring, deploying, operating, or otherwise participating in or facilitating a command and control infrastructure described in the TRO Application, including but not limited to the command and control software hosted at and operating through the Internet domains set forth in **Appendix A** and through any other component or element of the command and control infrastructure at any location; (4) stealing information from Plaintiffs, or their customers and members; (5) misappropriating that which rightfully belongs to Plaintiffs, their customers or

members, or in which Plaintiffs, their customers or members have a proprietary interest; (6) downloading or offering to download additional malicious software onto the computers of Plaintiffs, their customers or members; or (7) undertaking any similar activity that inflicts harm on Plaintiffs, their customers or members, or the public.

IT IS FURTHER ORDERED that, Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants are temporarily restrained and enjoined from (1) using and infringing Microsoft's trademarks, including specifically "Microsoft," bearing registration number 5449084, "Windows," bearing registration number 2463509 and serial number 90792752, "Excel," bearing registration numbers 2942050 and 85467589, "Word," bearing registration numbers 4355444 and 6148514 and/or other trademarks, trade names, service marks, or Internet Domain addresses or names; (2) using in connection with Defendants' activities, products, or services any false or deceptive designation, representation or description of Defendants or of their activities, whether by symbols, words, designs or statements, which would damage or injure Microsoft, or FS-ISAC's members or give Defendants an unfair competitive advantage or result in deception of consumers; or (3) acting in any other manner which suggests in any way that Defendants' activities, products or

services come from or are somehow sponsored by or affiliated with Microsoft or FS-ISAC's members, or passing off Defendants' activities, products or services as Microsoft's or FS-ISAC's members.

IT IS FURTHER ORDERED that, with respect to any currently registered Internet domains set forth in **Appendix A**, the domain registries shall take the following actions:

A. Within five (5) business days of receipt of this Order, shall unlock and change the registrar of record for the domain to MarkMonitor or such other registrar specified by Plaintiffs. To the extent the registrar of record does not assist in changing the registrar of record for the domain under its control, the domain registry for the domain, or its administrators, including backend registry operators or administrators, within five (5) business days of receipt of this Order, shall change, or assist in changing, the registrar of record for the domain to MarkMonitor or such other registrar specified by Plaintiffs. The purpose of this paragraph is to ensure that Plaintiffs have control over the hosting and administration of the domain in its registrar account at MarkMonitor or such other registrar specified by Plaintiffs. Plaintiffs shall provide to the domain registry or registrar of record any requested registrar information or account details necessary to effectuate the foregoing.

B. The domain shall be made active and shall resolve in the manner set forth in this order, or as otherwise specified by Plaintiffs, upon taking control of the domain;

C. The domain shall be redirected to secure servers by changing the authoritative name servers to ns081a.microsoftinternetsafety.net and ns081b.microsoftinternetsafety.net and taking other reasonable steps to work with Plaintiffs to ensure the redirection of the domain and to ensure that Defendants cannot use it to make unauthorized access to computers, infect computers, compromise computers and computer networks, monitor the owners and users of computers and computer networks, steal information from them or engage in any other activities prohibited by this order;

D. The WHOIS registrant, administrative, billing and technical contact and identifying information should be the following, or other information as may be specified by Plaintiffs:

Domain Administrator
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
United States
Phone: +1.4258828080
Facsimile: +1.4259367329
domains@microsoft.com

E. Prevent transfer, modification or deletion of the domain by

Defendants and prevent transfer or control of the domain to the account of any party other than Plaintiffs;

F. Take all steps required to propagate to the foregoing changes through the Domain Name System ("DNS"), including domain registrars.

IT IS FURTHER ORDERED that as soon as reasonably possible after the foregoing actions are taken by the domain registries or other appropriate internet authorities, Plaintiffs shall move the Court to unseal this case and make the appropriate portions of the filings in this action accessible to the public.

IT IS FURTHER ORDERED that copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint may be served by any means authorized by law, including (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to Defendants' domain registrars and/or hosting companies and as agreed to by Defendants in the domain registration and/or hosting agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent Defendants provided accurate contact information in the U.S.; and/or (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Defendants, to the extent Defendants provided accurate contact information in foreign countries that are signatories to such

treaties.

IT IS FURTHER ORDERED, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before this Court on **April 20, 2022 at 3:00 p.m.** to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against Defendants, enjoining Defendants from the conduct temporarily restrained by the preceding provisions of this Order.

IT IS FURTHER ORDERED that Plaintiffs shall post bond in the amount of $50,000 to be paid into the Court registry.

IT IS FURTHER ORDERED that Defendants shall file with the Court and serve on Plaintiffs' counsel any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later than one (1) day prior to the hearing on Plaintiffs' request for a preliminary injunction.

IT IS SO ORDERED this 8th day of April, 2022, at 10:15 AM.

Mark H. Cohen

MARK H. COHEN
UNITED STATES DISTRICT JUDGE

Exhibit 15

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

MICROSOFT CORPORATION, a Washington corporation, Plaintiff, v. JOHN DOES 1-2, CONTROLLING A COMPUTER NETWORK AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS Defendants.	Civil Action No. 1:22-cv-607 (AJT/WEF) **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5**

***EX PARTE* TEMPORARY RESTRAINING ORDER AND**
ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

Plaintiff Microsoft Corporation ("Microsoft") has filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) Trademark Infringement under the Lanham Act, 15 U.S.C. § 1114 *et seq.;* (3) False Designation of Origin under the Lanham Act, 15 U.S.C. § 1125(a); (4) Trademark Dilution under the Lanham Act, 15 U.S.C. § 1125(c)(5) Common Law Trespass to Chattels; (6) Unjust Enrichment; and (7) Conversion. Microsoft has moved *ex parte* for an emergency temporary restraining order and an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C. § 1116(a) (the Lanham Act), and 28 U.S.C. § 1651(a) (the All-Writs Act).

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Microsoft's *Ex Parle* Application for an Emergency Temporary Restraining

Order and Order to Show Cause re Preliminary Injunction, the Court hereby makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case, and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against Defendants John Doe 1-2 ("Defendants") under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Lanham Act (15 U.S.C. §§ 1114, 1125), the common law of trespass to chattels, unjust enrichment and conversion, pursuant to Defendants' breach of contract.

2. Microsoft has made a clear showing that it is likely to succeed on the merits of its claims that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Lanham Act (15 U.S.C. §§ 1114, 1125), and constitute trespass to chattels, unjust enrichment, conversion, and breach of contract, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. Microsoft owns the registered trademarks Microsoft, Microsoft corporate logo, OneDrive, Share Point and Office 365 and numerous other trademarks used in connection with its services, software and products. There is good cause to believe that, unless Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations. The evidence set forth in Microsoft's Brief in Support of *Ex Parte* Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Application"), and the accompanying declarations and exhibits, demonstrates that Microsoft is likely to prevail on its claim that Defendants have engaged in violations of the foregoing law by:

a. intentionally accessing and sending malicious software, code, and instructions to the protected computers, operating systems, and computer networks of Microsoft and the customers of Microsoft, without authorization or exceeding authorization, in order to

   i. steal and exfiltrate information from those computers and computer networks;

   ii. infect those computers and computer networks with malicious code and thereby gain control over those computers and computer networks;

   iii. attack and compromise the security of those computers and computer networks by conducting remote reconnaissance, stealing authentication credentials, monitoring the activities of users, and using other instrumentalities of theft;

b. deploying computers, Internet domains and IP addresses to establish a command and control infrastructure by which means Defendants conduct illegal activities, including attacks on computers and networks, monitoring activities of users, and theft of information;

c. corrupting Microsoft's applications on victims' computers and Microsoft's servers, thereby using them to monitor the activities of users and steal information from them;

4. Microsoft has made a clear showing that if such conduct continues, irreparable harm will occur to Microsoft, Microsoft's customers, and the public and that the Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court. In that regard, there is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of command and control software that is hosted at and otherwise operates through the Internet domains listed in **Appendix A** to this Order, and from the destruction or concealment of other discoverable evidence of Defendants' misconduct available via those domains, including on user computers infected by Defendants, if Defendants receive advance notice of this action. Based on the evidence cited in Microsoft's TRO Application

and accompanying declarations and exhibits, Microsoft is likely to be able to prove that:

a. Defendants are engaged in activities that directly violate United States law and harm Microsoft and the public, including Microsoft's customers;

b. Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests;

c. Defendants are likely to delete or to relocate the command and control software at issue in Microsoft's TRO Application and the harmful and malicious software disseminated through the Internet domains listed in **Appendix A,** thereby permitting them to continue their illegal acts; and

d. Defendants are likely to warn their associates engaged in such activities if informed of Microsoft's action.

5. Microsoft has made a sufficient showing that the balance of equities strongly favors granting their requested injunctive relief. Defendants can claim no legally cognizable harm because an injunction would only require Defendants to cease illegal activities while failure to grant an injunction would allow Microsoft and its customers to continue to be harmed by Defendants' conduct.

6. Microsoft has made a sufficient showing that granting injunctive relief is in the public interest. Granting injunctive relief would protect additional members of the public from falling victim to Defendants' illegal conduct and having their accounts, computers, and devices unlawfully hacked and their information stolen. Furthermore, the public interest is clearly served by enforcing statutes designed to protect the public

7. Microsoft's request for this emergency *ex parte* relief is not the result of any lack of diligence on Microsoft's part, but instead based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), 15 U.S.C. § 1116(a) and 28 U.S.C. § 1651(a), good cause and the interest of justice require that this

Order be Granted without prior notice to Defendants, and accordingly, Microsoft is relieved of the duty to provide Defendants with prior notice of Microsoft's motion.

8. There is good cause to believe that Defendants have operated their spearphishing campaigns through certain instrumentalities - specifically the domains and the domain registration facilities of the domain registries in Virginia identified in **Appendix A.**

9. There is good cause to believe that Defendants have engaged in illegal activity by using the domain registration facilities of the domain registries identified in **Appendix A** to register the Internet domains identified in **Appendix A,** and violated the trademarks of the Microsoft products so as to deceive Microsoft's customers to steal credentials for their Microsoft accounts, and to deliver from those domains the malicious code, content, and commands that Defendants use to access Microsoft's services without authorization and to receive the information stolen from those accounts and computers.

10. There is good cause to believe that Defendants have engaged in illegal activity by using deceptive and fraudulent methods to steal computer users' account credentials and to use such credentials for illegal purposes.

11. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants must be prohibited from accessing Microsoft's services without authorization and prohibited from sending malicious code, content and commands from the Internet domains identified in **Appendix A** to the computers of Microsoft's customers or to Microsoft's servers.

12. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains identified in **Appendix A** to host the malicious content used to

compromise the computers and servers of Microsoft and Microsoft's customers and to steal information from them. There is good cause to believe that to immediately halt the injury caused by Defendants, each of Defendants' domains set forth in **Appendix A** must be immediately transferred beyond the control of Defendants, thus making them inaccessible to Defendants.

13. There is good cause to believe that to immediately halt the injury, the execution of this Order should be carried out in a coordinated manner by Microsoft and by the domain registries identified in **Appendix A** on such date and time within five (5) days of this Order as may be reasonably requested by Microsoft.

14. There is good cause to believe that Defendants may change the Internet domains that they use to conduct illegal activities, and that Microsoft may identify and update the domains listed in **Appendix A** as may be reasonably necessary to account for additional Internet domains associated with Defendants just prior to the execution of this Order and within a reasonable time thereafter should Defendants attempt to evade and defy this Order.

15. There is good cause to permit notice of the instant Order, notice of the Preliminary Injunction hearing and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, and satisfy Fed. R. Civ. P. 4(t)(3) and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to Defendants' domain registrars and hosting companies and as agreed to by Defendants in

Defendants' domain registration and/or hosting agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent Defendants provided accurate contact information in the U.S.; and (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Defendants, to the extent Defendants provided accurate contact information in foreign countries that are signatories to such treaties.

TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

IT IS THEREFORE ORDERED that, Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants, are temporarily restrained and enjoined from: (I) intentionally accessing and sending malicious software or code to Microsoft and the protected computers and operating systems of Microsoft and Microsoft's customers, without authorization, in order to compromise those computers; (2) intentionally attacking and compromising computers or computer networks of Microsoft or Microsoft's customers, to monitor the activities of the owners or users of those computers or computer networks, and to steal information from those computers or networks; (3) configuring, deploying, operating, or otherwise participating in or facilitating infrastructure described in the TRO Application, including but not limited to the software hosted at and operating through the Internet domains set forth in **Appendix A** and through any other component or element of the Defendants' illegal infrastructure at any location; (4) stealing information from Microsoft's customers; (5) misappropriating that which rightfully belongs to Microsoft, its customers, or in which Microsoft or its customers have a proprietary interest; (6) downloading or offering to

download additional malicious software onto the computers of Microsoft's customers; or (7) undertaking any similar activity that inflicts harm on Microsoft, Microsoft's customers, or the public.

IT IS FURTHER ORDERED that, Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants are temporarily restrained and enjoined from (I) using and infringing Microsoft's trademarks, including specifically Microsoft's registered trademarks Microsoft, Microsoft corporate logo, OneDrive, SharePoint and Office 365 and/or other trademarks, trade names, service marks, or Internet Domain addresses or names containing or infringing such trademarks, trade names or service marks; (2) using in connection with Defendants' activities, products, or services any false or deceptive designation, representation or description of Defendants or of their activities, whether by symbols, words, designs or statements, which would damage or injure Microsoft or give Defendants an unfair competitive advantage or result in deception of consumers; or (3) acting in any other manner which suggests in any way that Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Microsoft, or passing off Defendants' activities, products or services as Microsoft's.

IT IS FURTHER ORDERED that, with respect to any currently registered Internet domains set forth in **Appendix A** to this Order, the domain registries located in the United States shall take the following actions:

A. Within five (5) business days of receipt of this Order, shall unlock and change the registrar of record for the domain to MarkMonitor or such other registrar

specified by Microsoft. To the extent the registrar of record does not assist in changing the registrar of record for the domain under its control, the domain registry for the domain, or its administrators, including backend registry operators or administrators, within five (5) business days of receipt of this Order, shall change, or assist in changing, the registrar of record for the domain to MarkMonitor or such other registrar specified by Microsoft. The purpose of this paragraph is to ensure that Microsoft has control over the hosting and administration of the domain in its registrar account at MarkMonitor or such other registrar specified by Microsoft. Microsoft shall provide to the domain registry or registrar of record any requested registrar information or account details necessary to effectuate the foregoing.

B. The WHOIS registrant, administrative, billing and technical contact and identifying information should be the following, or other information as may be specified by Microsoft:

Domain Administrator
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052 United States
Phone: +1.4258828080
Facsimile: +1.4259367329
domains@microsoft.com

C. Prevent transfer, modification or deletion of the domain by Defendants and prevent transfer or control of the domain to the account of any party other than Microsoft;

D. Take all steps required to propagate to the foregoing changes through the Domain Name System ("DNS"), including domain registrars.

2. With regard to the domain registries and registrars located outside of the United States, the Court respectfully requests, but does not order, that they take the same or substantially similar actions as the foregoing so as to neutralize the threat posed by the Defendants to the citizens of all countries, including their own. Defendants, their representatives and persons who are in active concert or participation with them are ordered to consent to whatever actions are necessary for non-United States registries, registrars and registrants or hosts, set forth in Appendix A, to effectuate this request.

IT IS FURTHER ORDERED that copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint may be served by any means authorized by law, including (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to Defendants' domain registrars and/or hosting companies and as agreed to by Defendants in the domain registration and/or hosting agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent Defendants provided accurate contact information in the U.S.; and (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Defendants, to the extent Defendants provided accurate contact information in foreign countries that are signatories to such treaties.

IT IS FURTHER ORDERED, pursuant to Federal Rule of Civil Procedure 65(b) that a hearing on Microsoft's Motion for a Preliminary Injunction is scheduled for June 10, 2022, at 10:00 am., in which it may request a preliminary injunction pending a final ruling on the Complaint against Defendants, enjoining Defendants from the conduct temporarily restrained by the preceding provisions of this Order.

IT IS FURTHER ORDERED that Microsoft shall post bond in the amount of $15,000 to be paid into the Court registry.

IT IS FURTHER ORDERED that Defendants shall file with the Court and serve on Microsoft's counsel any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later than one (1) day prior to the hearing on Microsoft's request for a preliminary injunction.

IT IS SO ORDERED

Entered this 27th day of May, 2022
at 11:30 a.m.

/s/
Anthony J. Trenga
United States District Judge
UNITED STATES DISTRICT JUDGE

Exhibit 16

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MICROSOFT CORPORATION, a Washington Corporation, FORTRA, LLC, a Minnesota Corporation, and HEALTH-ISAC, INC., a Florida Corporation,
Plaintiff,
v.

JOHN DOES 1-2, JOHN DOES 3-4 (AKA CONTI RANSOMWARE GROUP), JOHN DOES 5-6 (AKA LOCKBIT RANSOMWARE GROUP), JOHN DOES 7-8 (AKA DEV-0193), JOHN DOES 9-10 (AKA DEV-0206), JOHN DOES 11-12 (AKA DEV-0237), JOHN DOES 13-14 (AKA DEV-0243), JOHN DOES 15-16 (AKA DEV-0504), Controlling Computer Networks and Thereby Injuring Plaintiffs and Their Customers,

Defendants.

Case No. 23-cv-2447-LDH-JRC

FILED UNDER SEAL

***EX PARTE* TEMPORARY RESTRAINING ORDER, SEIZURE ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

Plaintiffs Microsoft Corp. ("Microsoft"), Fortra LLC ("Fortra"), and Health-ISAC, Inc. ("Health-ISAC") have filed a Complaint for injunctive and other relief pursuant to, Digital Millennium Copyright Act (17 U.S. § 1201); the Copyright Act (17 U.S.C. §§ 101 *et seq.*); the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); violations of the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); conspiracy to violate the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); and the common law of trespass, conversion, and unjust enrichment. Plaintiffs have also moved *ex parte* for an emergency temporary restraining order and seizure order pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C § 1116(d) (the "Lanham Act") and 28 U.S.C. § 1651(a) (the "All Writs Act"), and an order to show cause why a preliminary injunction should not be granted.

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Plaintiffs' Application for an Emergency Temporary Restraining Order, Seizure Order, and Order to Show Cause for Preliminary Injunction ("TRO Application"), the Court hereby makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against Defendants under the Digital Millennium Copyright Act (17 U.S. § 1201); the Copyright Act (17 U.S.C. §§ 101 *et seq.*); the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); violations of the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); conspiracy to violate the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); and the common law of trespass, conversion, and unjust enrichment.

2. Microsoft owns the registered trademarks "Microsoft" and "Windows" used in connection with its services, software, and products. Copies of the trademark registrations

for the Microsoft marks are attached as **Appendix B** to the Complaint.

3. Microsoft also owns copyrights in the code, documentation, specifications, libraries, and other materials that comprise the Windows operating system, including the Declaring Code (the code at issue in this case encompasses a type of code called "declarations" within header files and within libraries contained in the software development kit ("SDK")). Specifically, Microsoft owns the registered copyrights in the Windows 8 SDK, Reg. No. TX 8-999-365 (Copyrighted Work). Microsoft's Copyrighted Work is an original, creative work and copyrightable subject matter under the laws of the United States. Copies of the registration are attached to the Complaint as **Appendix C**.

4. Fortra also owns the copyrights in the code, documentation, specifications, libraries, and other materials that comprise the Cobalt Strike proprietary software. Fortra's copyrights are registered with the United States Copyright Office. Copies of the registration are attached to the Complaint as **Appendix D**.

5. Fortra owns the registered trademark in Cobalt Strike. Copies of the trademark registration for Fortra are attached to the Complaint as **Appendix E.**

6. Health-ISAC's members have invested in developing their brands, trademarks and trade names in association with the healthcare industry. Health-ISAC represents the interests of its members in maintaining security and maintaining their brand integrity regarding security matters.

7. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate Digital Millennium Copyright Act (17 U.S. § 1201); the Copyright Act (17 U.S.C. §§ 101 *et seq.*); the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); violations of the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); conspiracy to violate the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); and the common law of trespass, conversion, and unjust enrichment.

8. There is good cause to believe that, unless Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from Defendants' ongoing violations of the Digital Millennium Copyright Act (17 U.S. § 1201); the Copyright Act (17 U.S.C. §§ 101 *et seq.*); the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); violations of the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); conspiracy to violate the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); and the common law of trespass, conversion, and unjust enrichment. The evidence set forth in Plaintiffs' TRO Application and the accompanying declarations and exhibits, demonstrates that Plaintiffs are likely to prevail on their claim that Defendants have engaged in violations of the foregoing laws by: (1) using cracked versions of the Cobalt Strike software[1] to force their way into victim machines; (2) once inside the victims' machines, use unauthorized versions of Cobalt Strike to deploy ransomware and malware; (3) crippling victims' machines computer infrastructure and/or deleting files to force the payment of ransom from the victims; (4) stealing personal account information from users; (5) using the stolen personal information to carryout further illegal acts; (6) operate as a Ransom as a Service ("RaaS") model whereby affiliates pay to Defendants to launch ransomware attacks developed by other operators; and (7) associating with one another in a common enterprise engaged in these illegal acts. There is good cause to believe that if such conduct continues, irreparable harm will occur to Plaintiffs and the public, including Plaintiffs' customers and associated member organizations. There is good cause to believe that the Defendants are engaging, and will continue to engage, in such unlawful actions if not immediately restrained from doing so by Order of this Court.

9. There is good cause to believe that the malicious use of unauthorized Cobalt Strike software infringes Microsoft's copyright by copying literal lines of Microsoft Windows code, commands, system files, and file structures, and the structure, sequence, and organization of such code. For example, the malicious software's "beacon.dll" file copies literal code and the structure sequence and organization

[1] As used in this action, "cracked versions of Cobalt Strike" refer to stolen, unlicensed, or otherwise unauthorized versions or copies of Cobalt Strike.

of Windows code such as the GetUserObjectInformationA, RegCloseKey, LookupAccountSid, CryptGenRandom, LogonUserA, AdjustTokenPrivileges, ReadProcessMemory, TerminateProcess, CopyFileA, HttpSendRequestA code, and many other Windows code elements.

10. There is good cause to believe that the malicious use of unauthorized Cobalt Strike also infringes Fortra's copyright by literally copying the entirety of its copyrighted Cobalt Strike "team server" code in a cracked, unauthorized version used for malicious purposes. The infringement involves unauthorized copying of executable code for all of the Cobalt Strike team server's web server, beacon and configuration features and functionality, including all of Fortra's creative and original method implementations, interfaces, parameters, variables, arrays, data types, operators, and objects.

11. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of the unauthorized Cobalt Strike command and control ("C2") infrastructure that is hosted at and otherwise operates through the Internet domains listed in **Appendix A** or through the Internet Protocol ("IP") addressees, also listed in **Appendix A**, and from the destruction or concealment of other discoverable evidence of Defendants' misconduct available at those locations if Defendants receive advance notice of this action. Based on the evidence cited in Plaintiffs' TRO Application and accompanying declarations and exhibits, Plaintiffs are likely to be able to prove that: (1) Defendants are engaged in activities that directly violate U.S. law and harm Plaintiffs and the public, including Plaintiffs' customers and member-organizations; (2) Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests; (3) Defendants are likely to delete or relocate the command and control software at issue in Plaintiffs' TRO Application and the harmful, malicious, and trademark infringing software disseminated through these IP addresses and domains and to warn their associates engaged in such activities if informed of Plaintiffs' action. Plaintiffs' request for this emergency *ex parte* relief is not the result of any lack of diligence on Plaintiffs' part, but instead is based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b) and 15 U.S.C. § 1116(d), good cause and the interests of justice require that this Order be granted without prior notice to Defendants, and accordingly Plaintiffs are relieved of the duty to provide Defendants with prior notice of Plaintiffs' motion.

12. There is good cause to believe that Defendants have specifically directed their activities to computers of Plaintiffs' customers and member organization located in the Eastern District of New York.

13. There is good cause to believe that Defendants have engaged in illegal activity using the data centers and/or Internet hosting providers identified in Appendix A to host the unauthorized Cobalt Strike C2 infrastructure used to maintain and operate the unauthorized Cobalt Strike software at computers, servers, electronic data storage devices or media at the IP addresses identified in Appendix A.

14. There is good cause to believe that to immediately halt the injury caused by Defendants, data and evidence at Defendants' IP addresses identified in Appendix A must be preserved and held in escrow pending further order of the court, Defendants' computing resources related to such IP addresses must then be disconnected from Defendants' infrastructure, Defendants must be prohibited from accessing Defendants' computer resources related to such IP addresses and the data and evidence located on those computer resources must be secured and preserved.

15. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains identified in Appendix A to this order to host the command and control software and content used to maintain and operate the Defendants' harmful infrastructure. There is good cause to believe that to immediately halt the injury caused by Defendants, each of Defendants' current and prospective domains set forth in Appendix A must be immediately transferred to the control of Microsoft where they can be secured and thus made inaccessible to Defendants.

16. There is good cause to direct that third party Internet registries, registrars, data centers, and hosting providers with a presence in the United States to reasonably assist in the implementation of this Order and refrain from frustrating the implementation and purposes of this Order, pursuant to 28 U.S.C. § 1651(a) (the All Writs Act).

17. There is good cause to believe that if Defendants are provided advance notice of Plaintiffs' TRO Application or this Order, they would move the Defendants'

infrastructure, allowing them to continue their misconduct and that they would destroy, move, hide, conceal, or otherwise make inaccessible to the Court evidence of their misconduct, the Defendants' infrastructure's activity, the infringing materials, the instrumentalities used to make the infringing materials, and the records evidencing the manufacture and distributing of the infringing materials.

18. There is good cause to permit notice of the instant Order, notice of the Preliminary Injunction hearing and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, satisfy Fed. R. Civ. Pro. 4(f)(3), and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) personal delivery upon Defendants who provided to the data centers and Internet hosting providers contact information in the U.S.; (2) personal delivery through the Hague Convention on Service Abroad or other treaties upon Defendants who provided contact information outside the United States; (3) transmission by e-mail, electronic messaging addresses, facsimile, and mail to the known email and messaging addresses of Defendants and to their contact information provided by Defendants to the domain registrars, registries, data centers, Internet hosting providers, and website providers who host the software code associated with the IP addresses or through which domains are registered, both of which are identified in Appendix A.; and (4) publishing notice to the Defendants on a publicly available Internet website and in newspapers in jurisdictions where Defendants are believed to reside.

19. There is good cause to believe that the harm to Plaintiffs of denying the relief requested in their TRO Application outweighs any harm to any legitimate interests of Defendants and that there is no undue burden to any third party.

TEMPORARY RESTRAINING ORDER AND SEIZURE ORDER

IT IS THEREFORE ORDERED as follows:

A. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from: Using unauthorized versions of Cobalt Strike to brutally force access into victims' computers; using unauthorized versions of Cobalt Strike to operate a global malware and ransomware infrastructure, using unauthorized versions of Cobalt Strike to deploy malware and ransomware to victims' machines; using unauthorized version of Cobalt Strike to offer RaaS to other malicious actors; using the Conti and LockBit ransomware deployed via unauthorized Cobalt Strike to run and add its own protocols to the Microsoft operating system to go through the list of services and terminates services that are related to backup and recoveries as well as terminating security processes related to operating tool, which causes hundreds of lines of Microsoft's declaring code and the structure, sequence, and organization of that code are copied with and across unauthorized, cracked Cobalt Strike modules and ransomware like LockBit; using the infected victims' computers to send commands and instructions to the infected computing device to control it surreptitiously and deliver malware that, among other things, enables Defendants to take control of the victim's computer and extort money from them. Defendants' primary goal is to deliver ransomware and enable attacks against other computers; or stealing information, money or property from Plaintiffs, Plaintiffs' customers or Plaintiffs' member organizations, or undertaking any similar activity that inflicts harm on Plaintiffs, or the public, including Plaintiffs' customers or associated member organizations.

B. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from configuring, deploying, operating or otherwise using or unauthorized Cobalt Strike to facilitate the deployment of defendants' malware and ransomware activities described in the TRO Application, including but not limited to the C2 infrastructure hosted at and operating through the domains and IP addresses set forth herein and through any other deployments of unauthorized Cobalt Strike in any location.

C. Defendants, their representatives and persons who are in active concert or

participation with them are temporarily restrained and enjoined from using the trademarks or logos "Microsoft" or "Windows" the logos and trademarks "Cobalt Strike," the trademarks, brands or logos of healthcare institution members of Health-ISAC; and/or other trademarks; trade names; service marks; or Internet domain addresses or names; or acting in any other manner which suggests in any way that Defendants' products or services come from or are somehow sponsored or affiliated with Plaintiffs or Plaintiffs' associated member organizations, and from otherwise unfairly competing with Plaintiffs, misappropriating that which rightfully belongs to Plaintiffs or Plaintiffs' customers or Plaintiffs' associated member organizations, or passing off their goods or services as Plaintiffs or Plaintiffs' associated member organizations.

D. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from infringing Plaintiffs' registered trademarks, as set forth in Appendix B and E.

Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from using in connection with Defendants' activities any false or deceptive designation, representation or description of Defendants' or of their representatives' activities, whether by symbols, words, designs or statements, which would damage or injure Plaintiffs or give Defendants an unfair competitive advantage or result in deception of consumers.

IT IS FURTHER ORDERED, pursuant to the All Writs Act, with respect to any of the IP Addresses set forth in **Appendix A** to this Order, the data centers and/or hosting providers identified in **Appendix A** to this Order shall take reasonable best efforts to implement the following actions:

A. Take reasonable steps to identify incoming and/or outgoing Internet traffic on their respective networks associated with Defendants that originates and/or is being sent from and/or to the IP Addresses identified in Appendix A;

B. Take reasonable steps to block incoming and/or outgoing Internet traffic on

their respective networks associated with Defendants that originate and/or are being sent from and/or to the IP Addresses identified in Appendix A, by Defendants or Defendants' representatives or resellers, except as explicitly provided for in this Order;

C. Completely disable the computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with Defendants' use of the IP Addresses set forth in Appendix A and make them inaccessible from any other computer on the Internet, any internal network, or in any other manner, to Defendants, Defendants' representatives and all other persons, except as otherwise ordered herein;

D. Completely, and until further order of this Court, suspend all services to Defendants or Defendants' representatives or resellers associated with the IP Addresses set forth in Appendix A;

E. Isolate and disable any content and software associated with the Defendants hosted at the IP Addresses listed in Appendix A in a manner that does not impact any content or software not associated with Defendants hosted at the IP Addresses listed in Appendix A. In determining the method and mechanism to disable content and software associated with the Defendants, the relevant data centers and/or hosting providers shall reasonably confer with Plaintiffs' counsel, Gabriel M. Ramsey, Crowell & Moring LLP, 3 Embarcadero Ctr., 26th Floor, San Francisco, CA 94111, gramsey@crowell.com, (Tel: 415-365-7207), to facilitate any follow-on action;

F. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from publicizing this Order until this Order is executed in full, except as necessary to communicate with hosting companies, data centers, the Plaintiffs or other ISPs to execute this order;

G. Not enable, and shall take all reasonable steps to prevent, any circumvention of this order by Defendants or Defendants' representatives associated with the IP Addresses, including without limited to enabling, facilitating, and/or allowing Defendants or Defendants' representatives or resellers to rent, lease, purchase, or otherwise obtain another

IP Address associated with your services;

H. Preserve, retain and produce to Plaintiffs all documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or controlling the IP Addresses set forth in Appendix A, including any and all individual or entity names, mailing addresses, e-mail addresses, facsimile numbers and telephone numbers or similar contact information, including but not limited to such contact information reflected in billing, usage, access and contact records and all records, documents and logs associated with Defendants' or Defendants' Representatives' use of or access to the IP Addresses;

I. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order; and

J. Completely preserve the computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with the IP Addresses set forth in Appendix A, and preserve all evidence of any kind related to the content, data, software or accounts associated with such IP addresses and such computer hardware, such that such evidence of Defendants' unlawful activities is preserved.

IT IS FURTHER ORDERED that, pursuant to the All Writs Act, with respect to any currently registered Internet domain set forth in **Appendix A**, the domain registries shall take the following actions:

A. Within three (3) business days of receipt of this Order, shall unlock and change the registrar of record for the domain to MarkMonitor or such other registrar specified by Microsoft. To the extent the registrar of record does not assist in changing the registrar of record for the domain under its control, the domain registry for the domain, or its administrators, including backend registry operators or administrators, within five (5) business days of receipt of this Order, shall change, or assist in changing, the registrar of record for the domain to MarkMonitor or such other registrar specified by Microsoft. The purpose of this paragraph is to ensure that Microsoft has control over the hosting and administration of the domain in its registrar account at MarkMonitor or such other registrar specified by Microsoft. Microsoft shall

provide to the domain registry or registrar of record any requested registrar information or account details necessary to effectuate the foregoing.

B. The domain shall be made active and shall resolve in the manner set forth in this order, or as otherwise specified by Microsoft, upon taking control of the domain;

C. The domain registries shall take reasonable steps to work with Microsoft to ensure the transfer of the domain and to ensure that Defendants cannot use it to make unauthorized access to computers, infect computers, compromise computers and computer networks, monitor the owners and users of computers and computer networks, steal information from them or engage in any other activities prohibited by this Order;

D. The WHOIS registrant, administrative, billing and technical contact and identifying information should be the following, or other information as may be specified by Microsoft:

Domain Administrator
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
United States
Phone: +1.4258828080
Facsimile: +1.4259367329
domains@microsoft.com

E. Prevent transfer, modification or deletion of the domain by Defendants and prevent transfer or control of the domain to the account of any party other than Microsoft;

F. Take all steps required to propagate to the foregoing changes through the Domain Name System ("DNS"), including domain registrars.

IT IS FURTHER ORDERED that copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint may be served by any means authorized by law, including any one or combination of (1) personal delivery upon Defendants who provided accurate contact information in the U.S., if any; (2) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided accurate contact information in foreign countries that are signatory to such treaties, if any, (3) transmission by email, facsimile, mail and/or personal delivery to the contact information

provided by Defendants to their hosting companies and as agreed to by Defendants in their hosting agreements, (4) publishing notice on a publicly available Internet website and/or in newspapers in the communities where Defendants are believed to reside.

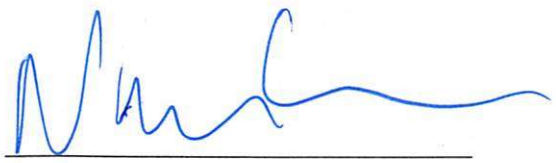
IT IS FURTHER ORDERED, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before the Hon. LaShann DeArcy Hall on April 13, 2023, at 1:00 p.m. to show cause, if there is any, why the Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against the Defendants, enjoining them from the conduct temporarily restrained by the preceding provisions of this Order.

IT IS FURTHER ORDERED that Microsoft, on behalf of Plaintiffs, shall post bond in the amount of $15,000 as cash to be paid into the Court registry.

IT IS FURTHER ORDERED that the Defendants shall file with the Court and serve on Plaintiffs' counsel any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later than two (2) days prior to the hearing on Plaintiffs' request for a preliminary injunction. Plaintiffs may file responsive or supplemental pleadings, materials, affidavits, or memoranda with the Court and serve the same on counsel for the Defendants no later than one (1) day prior to the preliminary injunction hearing in this matter. Provided that service shall be performed by personal or overnight delivery, facsimile or electronic mail, and documents shall be delivered so that they shall be received by the other parties no later than 4:00 p.m. (Eastern Standard Time) on the appropriate dates listed in this paragraph.

IT IS SO ORDERED

Entered this 31st day of March, 2023.



Hon. Nina R. Morrison, U.S.D.J.

(Miscellaneous Duty Judge)

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Microsoft Corporation, a Washington State Corporation, NGO-ISAC, a New York State Non-Profit Organization, Plaintiffs, v. John Does 1-2, Controlling A Computer Network and Thereby Injuring Plaintiff and Its Customers, Defendants.	Civil Action No. **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5.1**

[PROPOSED] *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

Plaintiffs Microsoft Corporation ("Microsoft") and NGO Information Sharing and Analysis Center ("NGO-ISAC") have filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) the Electronic Communications Privacy Act, 18 U.S.C. § 2701; (3) Trademark Infringement under the Lanham Act, 15 U.S.C. § 1114 *et seq*.; (4) False Designation of Origin under the Lanham Act, 15 U.S.C. § 1125(a); (5) Trademark Dilution under the Lanham Act, 15 U.S.C. § 1125(c) (6) Common Law Trespass to Chattels; (7) Conversion; and (8) Unjust Enrichment. Plaintiffs have moved *ex parte* for an emergency temporary restraining order and an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C. § 1116(a) (the Lanham Act), and 28 U.S.C. § 1651(a) (the All-Writs Act).

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Plaintiffs' *Ex Parte* Application for an Emergency Temporary Restraining Order and Order to

Show Cause re Preliminary Injunction, the Court hereby makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case, and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against Defendants John Doe 1-2 ("Defendants") under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), and the common law of trespass to chattels, conversion, and unjust enrichment.

2. There is good cause to believe that John Does 1-2 operate a sophisticated Russia-based, cybercriminal operation known as "Star Blizzard."

3. There is good cause to believe that Star Blizzard target Microsoft's customers, including NGO-ISAC and its member organizations, and the general public, that work to oppose the Russian government and are adverse to Russia's interests or global and domestic policy (such as its invasion of Ukraine).

4. There is good cause to believe that the Star Blizzard Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), and constitute trespass to chattels, conversion, and unjust enrichment, and Plaintiffs, therefore, are likely to prevail on the merits of this action.

5. Microsoft owns the registered trademarks Microsoft, Microsoft corporate logo, Outlook, OneDrive, Microsoft Word and Office 365 and numerous other trademarks used in connection with its services, software and products.

6. NGO-ISAC is an organization that has organizational standing to bring claims on

behalf of its member organization. NGO-ISAC's members, including the Carnegie Corporation of New York, owns registered trademarks in its names and logos used in connection with its nonprofit work.

7. There is good cause to believe that, unless the Star Blizzard Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Star Blizzard Defendants' ongoing violations. The evidence set forth in Plaintiffs' Brief in Support of *Ex Parte* Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Application"), and the accompanying declarations of Sean Ensz, Ian Gottesman, Yotaro Sherman, and Natalia Krapiva, and supporting exhibits, demonstrates that Plaintiffs are likely to prevail on its claim that the Star Blizzard Defendants have engaged in violations of the foregoing law by:

a. Intentionally accessing the protected computers and computer networks of Microsoft and the customers of Microsoft, including NGO-ISAC, and NGO-ISAC's member organizations, without authorization or exceeding authorization, in order to steal and exfiltrate information from those computers and computer networks;

b. Engaging in spear phishing operations to steal credentials from unsuspecting victims who are tricked into believing they are accessing legitimate websites;

c. Intentionally accessing, without authorization, the email inboxes of Microsoft customers, NGO-ISAC, NGO-ISAC's member organization in order to view and exfiltrate sensitive data including email contents, attachments to emails, and contact lists for the purpose of data theft;

d. Infringing the protected marks of Plaintiffs for the purpose of causing confusion or mistake, whereby the victims of the Star Blizzard Defendants' attacks mistakenly believe that such conduct is endorsed by Plaintiffs.

8. There is good cause to believe that if such conduct continues, irreparable harm will occur to Microsoft, Microsoft's customers, NGO-ISAC, NGO-ISAC's members, and the public. There is good cause to believe that the Star Blizzard Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court.

9. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by the Star Blizzard Defendants of command and control software that is hosted at and otherwise operates through the Internet domains listed in **Appendix A** to this Order, and from the destruction or concealment of other discoverable evidence of the Star Blizzard Defendants' misconduct available via those domains, including on user computers infected by the Star Blizzard Defendants, if they receive advance notice of this action. Based on the evidence cited in Plaintiffs' TRO Application and accompanying declarations and exhibits, Plaintiffs are likely to be able to prove that:

a. The Star Blizzard Defendants are engaged in activities that directly violate United States law and harm Microsoft, its customers, NGO-ISAC, its member organizations, and the public;

b. The Star Blizzard Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests;

c. The Star Blizzard Defendants are likely to delete or to relocate the command and control software at issue in Plaintiffs' TRO Application and the harmful and malicious software disseminated through the Internet domains listed in **Appendix A**, thereby permitting them to continue their illegal acts; and

d. The Star Blizzard Defendants are likely to warn their associates engaged in such activities if informed of Plaintiffs' action.

10. Plaintiffs' request for this emergency *ex parte* relief is not the result of any lack of diligence on Plaintiffs' part, but instead, is based upon the nature of the Star Blizzard Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), 15 U.S.C. § 1116(a) and 28 U.S.C. § 1651(a), good cause and the interest of justice require that this Order be **Granted** without prior notice to the Star Blizzard Defendants, and accordingly, Plaintiffs are relieved of the duty to provide the Star Blizzard Defendants with prior notice of Plaintiffs' motion and requested relief.

11. There is good cause to believe that the Star Blizzard Defendants have operated their spearphishing campaigns through certain instrumentalities – specifically through the website domains identified in **Appendix A**.

12. There is good cause to believe that the Star Blizzard Defendants have (i) engaged in illegal activity by using the domain registration facilities of the domain registries identified in **Appendix A,** to register the Internet domains identified in **Appendix A**, (ii) violated Plaintiffs' trademarks in order to: (iii) deceive Plaintiffs' customers to steal credentials for their email accounts, infiltrate the email systems, and have unfettered access to the contents of those email accounts for purposes of data exfiltration.

13. There is good cause to believe that the Star Blizzard Defendants have engaged in illegal activity by using deceptive and fraudulent methods to steal computer users' account credentials and to use such credentials for illegal purposes.

14. There is good cause to believe that to immediately halt the injury caused by the Blizzard Defendants, they must be prohibited from accessing Plaintiffs' services without authorization, prohibited from the unlawful intrusion and data theft of the victims' email accounts, from using Plaintiffs' marks to perpetrate their unlawful and criminal scheme, and prevented from using the Internet domains identified in **Appendix A** to operate the command and control infrastructure to further its spear phishing operation.

15. There is good cause to believe that the Star Blizzard Defendants have engaged in illegal activity using the Internet domains identified in **Appendix A** to carry out their illegal spear phishing campaign. There is good cause to believe that to immediately halt the injury caused by the Star Blizzard Defendants, each of Star Blizzard's domains set forth in **Appendix A** must be immediately transferred beyond the control of the Star Blizzard criminal operation, thus making

them inaccessible to the Star Blizzard Defendants.

16. There is good cause to believe that to immediately halt the injury, the execution of this Order should be carried out in a coordinated manner by Plaintiffs and by the domain registries identified in **Appendix A** on such date and time within five (5) days of this Order as may be reasonably requested by Plaintiffs.

17. There is good cause to believe that the Star Blizzard Defendants have specifically directed their activities in the District of Columbia.

18. There is good cause to believe that if the Star Blizzard Defendants are provided advance notice of Plaintiffs' TRO Application or this Order, they would move the Star Blizzard Defendants' infrastructure, allowing them to continue their misconduct and that they would destroy, move, hide, conceal, or otherwise make inaccessible to the Court evidence of their misconduct, the Star Blizzard Defendants' infrastructure's activity, the infringing materials, the instrumentalities used to make the infringing materials, and the records evidencing the manufacture and distributing of the infringing materials.

19. There is good cause to permit notice of the instant Order, notice of the Preliminary Injunction hearing and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, and satisfy Fed. R. Civ. P. 4(f)(3) and are reasonably calculated to notify the Star Blizzard Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by the Star Blizzard Defendants to the Star Blizzard Defendants' domain registrars and hosting companies and as agreed to by the Star Blizzard Defendants in their domain registration and/or hosting agreements, (2) publishing notice on a publicly available

Internet website, (3) by personal delivery upon the Star Blizzard Defendants, to the extent the Star Blizzard Defendants provided accurate contact information in the U.S.; and (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon the Star Blizzard Defendants, to the extent the Star Blizzard Defendants provided accurate contact information in foreign countries that are signatories to such treaties.

20. There is good cause to believe that the Star Blizzard Defendants have no legitimate interest in carryout their cybercriminal activities.

21. There is good cause to believe that the harm to Plaintiffs in denying the relief requested in their TRO Application outweighs any harm to any legitimate interest of the Star Blizzard Defendants (of which there is none) and that there is no undue burden to any third party.

TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

IT IS THEREFORE ORDERED that, the Star Blizzard Defendants, their representatives, and persons who are in active concert or participation with the Star Blizzard Defendants and associated criminal operation, are temporarily restrained and enjoined from: (1) intentionally accessing the protected computers without authorization, (2) engaging in spear phishing campaigns, (3) stealing credentials from victims of spear phishing campaigns, (4) using the credentials to access the email inboxes of victims, (4) unlawfully accessing, viewing, exfiltrating, or otherwise stealing the contents of the compromised email inboxes, (5) capitalizing on the trademarks of Plaintiffs to fabricate legitimacy of the spear phishing campaign, (6) misappropriating that which rightfully belongs to Microsoft, its customers, or in which Microsoft or its customers have a proprietary interest; (7) destroying the goodwill and reputation of Plaintiffs, (8) impersonating Plaintiffs, their systems, products, and services, (9) configuring, deploying, operating, or otherwise participating in or facilitating infrastructure described in the TRO

Application, including but not limited to the Internet domains set forth in **Appendix A** and through any other component or element of the Star Blizzard Defendants' illegal infrastructure at any location, including infrastructure that the Star Blizzard Defendants may attempt to rebuild, and (10) undertaking any similar activity that inflicts harm on Microsoft, Microsoft's customers, NGO-ISAC, its member organizations, or the public.

IT IS FURTHER ORDERED that, the Star Blizzard Defendants, their representatives, and persons who are in active concert or participation with the Star Blizzard Defendants and associated criminal operation are temporarily restrained and enjoined from (1) using and infringing Plaintiffs' trademarks, including specifically Microsoft's registered trademarks Microsoft, Microsoft corporate logo, OneDrive, Outlook, Microsoft Word and Office 365 and the trademarks of NGO-ISAC's member organizations, including specifically Carnegie Corporation's register trademarks Carnegie Corporation of New York and its corporate logo, and/or other trademarks, trade names, service marks, or Internet domain addresses or names containing or infringing such trademarks, trade names or service marks, as set forth in **Appendix B and C** to this Order; (2) using in connection with the Star Blizzard Defendants' activities, products, or services any false or deceptive designation, representation or description of the Star Blizzard Defendants or of their activities, whether by symbols, words, designs or statements, which would damage or injure Plaintiffs or give the Star Blizzard Defendants an unfair competitive advantage or result in deception of consumers; or (3) acting in any other manner which suggests in any way that the Star Blizzard Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Plaintiffs, or passing off the Star Blizzard Defendants' activities, products or services as Plaintiffs'.

IT IS FURTHER ORDERED that, with respect to any currently registered Internet

domains set forth in **Appendix A** to this Order, the domain registries located in the United States shall take the following actions:

A. Within three (3) business days of receipt of this Order, shall unlock and change the registrar of record for the domain to MarkMonitor or such other registrar specified by Microsoft. To the extent the registrar of record does not assist in changing the registrar of record for the domain under its control, the domain registry for the domain, or its administrators, including backend registry operators or administrators, within three (3) business days of receipt of this Order, shall change, or assist in changing, the registrar of record for the domain to MarkMonitor or such other registrar specified by Microsoft. The purpose of this paragraph is to ensure that Microsoft has control over the hosting and administration of the domain in its registrar account at MarkMonitor or such other registrar specified by Microsoft. Microsoft shall provide to the domain registry or registrar of record any requested information or account details necessary to effectuate the foregoing.

B. The domain registries shall be made active and shall resolve in the manner set forth in this order, or as otherwise specified by Microsoft, upon taking control of the domain.

C. The domain registries shall take reasonable steps to work with Microsoft to ensure the transfer of the domain and to ensure that the Star Blizzard Defendants cannot use it to make unauthorized access to computers, infect computers, compromise computers and computer networks, monitor the owners and users of computers and computer networks, steal information from them, or engage in any other activities prohibited by this Order;

D. The WHOIS registrant, administrative, billing and technical contact and identifying information should be the following, or other information as may be specified by Microsoft:

Domain Administrator
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
United States
Phone: +1.4258828080
Facsimile: +1.4259367329
domains@microsoft.com

E. Prevent transfer, modification or deletion of the domain by the Star Blizzard Defendants and prevent transfer or control of the domain to the account of any party other than Microsoft;

F. Take all steps required to propagate to the foregoing changes through the Domain Name System ("DNS"), including domain registrars.

2. With regard to the domain registries and registrars located outside of the United States, the Court respectfully requests, but does not order, that they take the same or substantially similar actions as the foregoing so as to neutralize the threat posed by the Star Blizzard Defendants to the citizens of all countries, including their own. The Star Blizzard Defendants, their representatives and persons who are in active concert or participation with them are ordered to consent to whatever actions are necessary for non-United States registries, registrars and registrants or hosts, set forth in **Appendix A** to this Order, to effectuate this request.

IT IS FURTHER ORDERED that copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint may be served by any means authorized by law, including (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by the Star Blizzard Defendants to their domain registrars and/or hosting companies and as agreed to by the Star Blizzard Defendants in the domain registration and/or hosting agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent the Star Blizzard Defendants provided accurate contact

information in the U.S.; and (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon the Star Blizzard Defendants, to the extent they provided accurate contact information in foreign countries that are signatories to such treaties.

IT IS FURTHER ORDERED, pursuant to Federal Rule of Civil Procedure 65(b) that the Star Blizzard Defendants shall appear before this Court on October 8, 2024 at 9:00 a.m., to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against the Star Blizzard Defendants, enjoining the Star Blizzard Defendants from the conduct temporarily restrained by the preceding provisions of this Order.

IT IS FURTHER ORDERED that Microsoft, on behalf of Plaintiffs, shall post bond in the amount of $15,000 to be paid into the Court registry.

IT IS FURTHER ORDERED that the Star Blizzard Defendants shall file with the Court and serve on Plaintiffs' any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later than two (2) days prior to the hearing on Plaintiffs' request for a preliminary injunction. Plaintiffs may file responsive or supplemental pleadings, materials, affidavits, or memoranda with the Court and serve the same on counsel for the Star Blizzard Defendants no later than one (1) day prior to the preliminary injunction hearing in this matter. Provided that service shall be performed by personal or overnight delivery, facsimile or electronic mail, and documents shall be delivered so that they shall be received by the other parties no later than 4:00 p.m. (Eastern Standard Time) on the appropriate dates listed in this paragraph.

IT IS SO ORDERED

Entered this ____ day of September, 2024

UNITED STATES DISTRICT JUDGE

APPENDIX A

APPENDIX A

.COM REGISTRY
VeriSign Global Registry Services
12061 Bluemont Way
Reston VA 20190

.COM DOMAIN

ANKARAMUHASEBEN.COM	Domain Name: ANKARAMUHASEBEN.COM Registry Domain ID: 2859614504_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2024-02-29T16:32:16Z Creation Date: 2024-02-29T16:32:13Z Registry Expiry Date: 2025-02-28T16:32:13Z Registrar: NameCheap, Inc. Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: DNS1.REGISTRAR-SERVERS.COM Name Server: DNS2.REGISTRAR-SERVERS.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2024-09-20T17:17:01Z <<<
BIGDATABROADWAY.COM	Domain name: BIGDATABROADWAY.COM Registry Domain ID: 2856022843_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2024-02-17T18:27:19.00Z Registrar Registration Expiration Date: 2025-02-17T18:27:19.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy

	Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: cad10b04e802496cb7f315f443084ac1.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: cad10b04e802496cb7f315f443084ac1.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: cad10b04e802496cb7f315f443084ac1.protect@withheldforprivacy.com

	Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-20T16:20:25.39Z <<<
CLOUDDEFSYSTEMS.COM	Domain name: clouddefsystems.com Registry Domain ID: 2764044774_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-03-10T08:39:33.00Z Registrar Registration Expiration Date: 2024-03-10T08:39:33.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 94ac459a70de4e3bb65db311eea9da56.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region

	Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 94ac459a70de4e3bb65db311eea9da56.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 94ac459a70de4e3bb65db311eea9da56.protect@withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ For more information on Whois status codes, please visit https://icann.org/epp
CLOUDINFODATA.COM	Domain name: cloudinfodata.com Registry Domain ID: 2781367380_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-05-16T15:23:52.00Z Registrar Registration Expiration Date: 2024-05-16T15:23:52.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC

	Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: REACTIVATION PERIOD Registrant Organization: Withheld for Privacy Purposes Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: reactivation-pending@mail.withheldforprivacy.com Registry Admin ID: Admin Name: REACTIVATION PERIOD Admin Organization: Withheld for Privacy Purposes Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: reactivation-pending@mail.withheldforprivacy.com Registry Tech ID: Tech Name: REACTIVATION PERIOD Tech Organization: Withheld for Privacy Purposes Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: reactivation-pending@mail.withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com

	DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ For more information on Whois status codes, please visit https://icann.org/epp
CLOUDITHUB.COM	omain name: cloudithub.com Registry Domain ID: 2784305716_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2024-06-26T01:43:42.64Z Creation Date: 2023-05-26T16:28:35.00Z Registrar Registration Expiration Date: 2025-05-26T16:28:35.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 723eed6a6b98418d905c68cebf3d06be.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS

	Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 723eed6a6b98418d905c68cebf3d06be.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 723eed6a6b98418d905c68cebf3d06be.protect@withheldforprivacy.com Name Server: ns1.dan.com Name Server: ns2.dan.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ For more information on Whois status codes, please visit https://icann.org/epp
DATAWEBHUB.COM	Domain name: datawebhub.com Registry Domain ID: 2784305714_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2024-06-26T01:46:46.46Z Creation Date: 2023-05-26T16:28:34.00Z Registrar Registration Expiration Date: 2025-05-26T16:28:34.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

	Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: bb1402f4bbb14246947e77ef4598aae0.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: bb1402f4bbb14246947e77ef4598aae0.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext:

	Tech Email: bb1402f4bbb14246947e77ef4598aae0.protect@withheldforprivacy.com Name Server: ns1.dan.com Name Server: ns2.dan.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
DOCSECGATE.COM	Domain Name: DOCSECGATE.COM Registry Domain ID: 2797453581_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2024-08-22T13:39:52Z Creation Date: 2023-07-11T13:27:59Z Registry Expiry Date: 2024-07-11T13:27:59Z Registrar: NameCheap, Inc. Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: redemptionPeriod https://icann.org/epp#redemptionPeriod Name Server: DNS101.REGISTRAR-SERVERS.COM Name Server: DNS102.REGISTRAR-SERVERS.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2024-09-20T17:25:49Z <<<
E-FLUXXSOLUTIONS.COM	Domain name: e-fluxxsolutions.com Registry Domain ID: 2775421497_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-04-24T10:42:21.00Z Registrar Registration Expiration Date: 2024-04-24T10:42:21.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC

	Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: b115c8ed61ca4385bde370956ce374d8.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: b115c8ed61ca4385bde370956ce374d8.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax:

	Tech Fax Ext: Tech Email: b115c8ed61ca4385bde370956ce374d8.protect@withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ For more information on Whois status codes, please visit https://icann.org/epp
ENTHEOGENICMD.COM	Domain Name: ENTHEOGENICMD.COM Registry Domain ID: 2894098537_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.hostinger.com Registrar URL: http://www.hostinger.com Updated Date: 2024-06-26T13:54:05Z Creation Date: 2024-06-26T13:53:58Z Registry Expiry Date: 2025-06-26T13:53:58Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636 Registrar Abuse Contact Email: abuse-tracker@hostinger.com Registrar Abuse Contact Phone: +37064503378 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: NS1.DNS-PARKING.COM Name Server: NS2.DNS-PARKING.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2024-09-20T17:30:06Z <<<
EXTRACTORDRAW.COM	Domain Name: EXTRACTORDRAW.COM Registry Domain ID: 2863506875_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.hostinger.com Registrar URL: http://www.hostinger.com Updated Date: 2024-03-14T17:31:07Z Creation Date: 2024-03-14T17:31:02Z Registry Expiry Date: 2025-03-14T17:31:02Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636 Registrar Abuse Contact Email: abuse-tracker@hostinger.com Registrar Abuse Contact Phone: +37064503378

	Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: NS1.DNS-PARKING.COM Name Server: NS2.DNS-PARKING.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2024-09-20T17:31:22Z <<<
GALETSCRYPTODATA.COM	Domain name: galetscryptodata.com Registry Domain ID: 2760849968_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-02-24T18:49:12.00Z Registrar Registration Expiration Date: 2024-02-24T18:49:12.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 1938c38cd84245458600905600 2f69dc.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf

	Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 1938c38cd84245458600905600 2f69dc.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 1938c38cd84245458600905600 2f69dc.protect@withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ For more information on Whois status codes, please visit https://icann.org/epp
GATEBLURBREPOSITORY.COM	Domain Name: GATEBLURBREPOSITORY.COM Registry Domain ID: 2759139284_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2024-08-24T22:01:34Z Creation Date: 2023-02-17T18:02:46Z Registry Expiry Date: 2025-02-17T18:02:46Z Registrar: NameCheap, Inc. Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com

	Registrar Abuse Contact Phone: +1.6613102107 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: NS1.DAN.COM Name Server: NS2.DAN.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2024-09-20T17:35:56Z <<<
GATEWAYDOCSINT.COM	Domain name: gatewaydocsint.com Registry Domain ID: 2754772928_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-01-29T21:32:39.00Z Registrar Registration Expiration Date: 2025-01-29T21:32:39.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Redacted for Privacy Purposes Registrant Name: Redacted for Privacy Purposes Registrant Organization: Redacted for Privacy Purposes Registrant Street: Redacted for Privacy Purposes Registrant City: Redacted for Privacy Purposes Registrant State/Province: FL Registrant Postal Code: Redacted for Privacy Purposes Registrant Country: US Registrant Phone: Redacted for Privacy Purposes Registrant Phone Ext: Redacted for Privacy Purposes Registrant Fax: Redacted for Privacy Purposes Registrant Fax Ext: Redacted for Privacy Purposes Registrant Email: Select Contact Domain Holder link at https://www.namecheap.com/domains/whois/result?domain=gatewaydocsint.com Registry Admin ID: Redacted for Privacy Purposes Admin Name: Redacted for Privacy Purposes Admin Organization: Redacted for Privacy Purposes Admin Street: Redacted for Privacy Purposes Admin City: Redacted for Privacy Purposes

	Admin State/Province: Redacted for Privacy Purposes Admin Postal Code: Redacted for Privacy Purposes Admin Country: Redacted for Privacy Purposes Admin Phone: Redacted for Privacy Purposes Admin Phone Ext: Redacted for Privacy Purposes Admin Fax: Redacted for Privacy Purposes Admin Fax Ext: Redacted for Privacy Purposes Admin Email: Select Contact Domain Holder link at https://www.namecheap.com/domains/whois/result?domain=gatewaydocsint.com Registry Tech ID: Redacted for Privacy Purposes Tech Name: Redacted for Privacy Purposes Tech Organization: Redacted for Privacy Purposes Tech Street: Redacted for Privacy Purposes Tech City: Redacted for Privacy Purposes Tech State/Province: Redacted for Privacy Purposes Tech Postal Code: Redacted for Privacy Purposes Tech Country: Redacted for Privacy Purposes Tech Phone: Redacted for Privacy Purposes Tech Phone Ext: Redacted for Privacy Purposes Tech Fax: Redacted for Privacy Purposes Tech Fax Ext: Redacted for Privacy Purposes Tech Email: Select Contact Domain Holder link at https://www.namecheap.com/domains/whois/result?domain=gatewaydocsint.com Name Server: ns1.dan.com Name Server: ns2.dan.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-19T22:38:23.64Z <<<
GAWECRYPTOINFOSOLUTIONS.COM	Domain name: gawecryptoinfosolutions.com Registry Domain ID: 2760849980_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-02-24T18:49:17.00Z Registrar Registration Expiration Date: 2024-02-24T18:49:17.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC

	Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 820478c363754e72bad77cc0e5a20663.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 820478c363754e72bad77cc0e5a20663.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax:

	Tech Fax Ext: Tech Email: 820478c363754e72bad77cc0e5a20663.protect@withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ For more information on Whois status codes, please visit https://icann.org/epp
GETFIGMACREATOR.COM	Domain name: GETFIGMACREATOR.COM Registry Domain ID: 2805036851_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-08-11T13:13:20.00Z Registrar Registration Expiration Date: 2024-08-11T13:13:20.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: REACTIVATION PERIOD Registrant Organization: Withheld for Privacy Purposes Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: reactivation-pending@mail.withheldforprivacy.com Registry Admin ID: Admin Name: REACTIVATION PERIOD Admin Organization: Withheld for Privacy Purposes Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik

	Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: reactivation-pending@mail.withheldforprivacy.com Registry Tech ID: Tech Name: REACTIVATION PERIOD Tech Organization: Withheld for Privacy Purposes Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: reactivation-pending@mail.withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-19T18:41:32.94Z <<<
GOVSAFEBREAKTHROUGH.COM	Domain name: GOVSAFEBREAKTHROUGH.COM Registry Domain ID: 2797988434_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-07-13T16:26:44.00Z Registrar Registration Expiration Date: 2024-07-13T16:26:44.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

	Domain Status: pendingDelete https://icann.org/epp#pendingDelete Domain Status: redemptionPeriod https://icann.org/epp#redemptionPeriod Registry Registrant ID: Registrant Name: REACTIVATION PERIOD Registrant Organization: Withheld for Privacy Purposes Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: reactivation-pending@mail.withheldforprivacy.com Registry Admin ID: Admin Name: REACTIVATION PERIOD Admin Organization: Withheld for Privacy Purposes Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: reactivation-pending@mail.withheldforprivacy.com Registry Tech ID: Tech Name: REACTIVATION PERIOD Tech Organization: Withheld for Privacy Purposes Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: reactivation-pending@mail.withheldforprivacy.com

	Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-20T16:43:20.59Z <<<
GUARDITTECH.COM	Domain name: guarditttech.com Registry Domain ID: 2772370916_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-04-12T13:36:33.00Z Registrar Registration Expiration Date: 2024-04-12T13:36:33.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 7c57f044c47e45b5a673950a7861ba8b.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region

	Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 7c57f044c47e45b5a673950a7861ba8b.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 7c57f044c47e45b5a673950a7861ba8b.protect@withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ For more information on Whois status codes, please visit https://icann.org/epp
HELMETKUP.COM	Domain name: HELMETKUP.COM Registry Domain ID: 2859617771_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2024-02-29T17:04:27.00Z Registrar Registration Expiration Date: 2025-02-28T17:04:27.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC

	Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: b0f651910fc24e5cb826549a09331910.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: b0f651910fc24e5cb826549a09331910.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax:

	Tech Fax Ext: Tech Email: b0f651910fc24e5cb826549a09331910.protect@withheldforprivacy.com Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-20T09:44:28.70Z <<<
IMGRICH.COM	Domain Name: IMGRICH.COM Registry Domain ID: 2863761839_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.hostinger.com Registrar URL: http://www.hostinger.com Updated Date: 2024-03-15T14:56:16Z Creation Date: 2024-03-15T14:56:13Z Registry Expiry Date: 2025-03-15T14:56:13Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636 Registrar Abuse Contact Email: abuse-tracker@hostinger.com Registrar Abuse Contact Phone: +37064503378 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: NS1.DNS-PARKING.COM Name Server: NS2.DNS-PARKING.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2024-09-20T17:48:02Z <<<
INREALCONNECT.COM	Domain Name: INREALCONNECT.COM Registry Domain ID: 2870766541_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2024-04-09T14:49:24Z Creation Date: 2024-04-09T14:49:21Z Registry Expiry Date: 2025-04-09T14:49:21Z Registrar: NameCheap, Inc. Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107

	Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: DNS1.REGISTRAR-SERVERS.COM Name Server: DNS2.REGISTRAR-SERVERS.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2024-09-20T17:49:04Z <<<
INSTANTPOINTZERO.COM	Domain name: INSTANTPOINTZERO.COM Registry Domain ID: 2861020667_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2024-03-05T12:37:50.00Z Registrar Registration Expiration Date: 2025-03-05T12:37:50.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 9165fd17e3a24cedb27207ac20cbb972.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy

	Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 9165fd17e3a24cedb27207ac20cbb972.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 9165fd17e3a24cedb27207ac20cbb972.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-20T06:52:04.76Z <<<
INTELLIGENTAUTOMATIONALLEY.COM	Domain name: INTELLIGENTAUTOMATIONALLEY.COM Registry Domain ID: 2856020497_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2024-02-17T17:57:50.00Z

	Registrar Registration Expiration Date: 2025-02-17T17:57:50.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: e7c4de7cd08642b3a8c409c734a647d8.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: e7c4de7cd08642b3a8c409c734a647d8.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2

	Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: e7c4de7cd08642b3a8c409c734a647d8.protect@withheldforprivacy.com Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-20T02:54:16.18Z <<<
KEEPERDOCUMENTLLC.COM	Domain name: keeperdocumentllc.com Registry Domain ID: 2765526386_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-03-16T09:09:23.00Z Registrar Registration Expiration Date: 2024-03-16T09:09:23.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax:

	Registrant Fax Ext: Registrant Email: 242400c85b41476d846e8cc4a0b8f62d.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 242400c85b41476d846e8cc4a0b8f62d.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 242400c85b41476d846e8cc4a0b8f62d.protect@withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ For more information on Whois status codes, please visit https://icann.org/epp
KEEPERITLABEL.COM	Domain name: keeperitlabel.com

	Registry Domain ID: 2762230896_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-03-02T16:03:10.00Z Registrar Registration Expiration Date: 2024-03-02T16:03:10.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 75fa2915399b4e47abcf39c76a78b44f.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext:

	Admin Email: 75fa2915399b4e47abcf39c76a78b44f.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 75fa2915399b4e47abcf39c76a78b44f.protect@withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ For more information on Whois status codes, please visit https://icann.org/epp
LIQUIDACIONESJUDICIALES.COM	Domain Name: liquidacionesjudiciales.com Registry Domain ID: 2760466030_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.regtons.com Registrar URL: http://regtons.com Updated Date: 2024-02-23T00:00:00Z Creation Date: 2023-02-22T00:00:00Z Registrar Registration Expiration Date: 2025-02-22T00:00:00Z Registrar: GRANSY S.R.O D/B/A SUBREG.CZ Registrar IANA ID: 1505 Registrar Abuse Contact Email: abuse@regtons.com Registrar Abuse Contact Phone: +420.734463373 Domain Status: clienttransferprohibited https://www.icann.org/epp#clienttransferprohibited Registry Registrant ID: Not Disclosed Registrant Name: Not Disclosed Not Disclosed Registrant Organization: My Domain Provider Registrant Street: Not Disclosed Registrant City: Not Disclosed

	Registrant State/Province: Registrant Postal Code: Not Disclosed Registrant Country: NL Registrant Phone: Not Disclosed Registrant Phone Ext: Not Disclosed Registrant Fax: Not Disclosed Registrant Fax Ext: Not Disclosed Registrant Email: webproxy@whoisprotection.domains Registry Admin ID: Not Disclosed Admin Name: Not Disclosed Not Disclosed Admin Organization: Admin Street: Not Disclosed Admin City: Not Disclosed Admin State/Province: Not Disclosed Admin Postal Code: Not Disclosed Admin Country: Not Disclosed Admin Phone: Not Disclosed Admin Phone Ext: Not Disclosed Admin Fax: Not Disclosed Admin Fax Ext: Not Disclosed Admin Email: webproxy@whoisprotection.domains Registry Tech ID: Not Disclosed Tech Name: Not Disclosed Not Disclosed Tech Organization: Tech Street: Not Disclosed Tech City: Not Disclosed Tech State/Province: Not Disclosed Tech Postal Code: Not Disclosed Tech Country: Not Disclosed Tech Phone: Not Disclosed Tech Phone Ext: Not Disclosed Tech Fax: Not Disclosed Tech Fax Ext: Not Disclosed Tech Email: webproxy@whoisprotection.domains Name Server: suspension1.mydomainprovider.com Name Server: suspension2.mydomainprovider.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
MAYQUARKESTHETIC.COM	Domain Name: MAYQUARKESTHETIC.COM Registry Domain ID: 2870492494_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.hostinger.com Registrar URL: https://www.hostinger.com Updated Date: 2024-06-08T02:17:53Z Creation Date: 2024-04-08T17:00:35Z

	Registrar Registration Expiration Date: 2025-04-08T17:00:35Z Registrar: Hostinger Operations, UAB Registrar IANA ID: 1636 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: 10 Corporate Drive Registrant City: Burlington Registrant State/Province: MA Registrant Postal Code: 01803 Registrant Country: US Registrant Phone: +1.8022274003 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@privacyprotect.org Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: Privacy Protect, LLC (PrivacyProtect.org) Admin Street: 10 Corporate Drive Admin City: Burlington Admin State/Province: MA Admin Postal Code: 01803 Admin Country: US Admin Phone: +1.8022274003 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact@privacyprotect.org Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: Privacy Protect, LLC (PrivacyProtect.org) Tech Street: 10 Corporate Drive Tech City: Burlington Tech State/Province: MA Tech Postal Code: 01803 Tech Country: US Tech Phone: +1.8022274003 Tech Phone Ext: Tech Fax:

	Tech Fax Ext: Tech Email: contact@privacyprotect.org Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse@hostinger.com Registrar Abuse Contact Phone: +37064503378 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
METTEZERA.COM	Domain Name: METTEZERA.COM Registry Domain ID: 2894114626_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.hostinger.com Registrar URL: https://www.hostinger.com Updated Date: 2024-08-26T02:17:11Z Creation Date: 2024-06-26T16:33:04Z Registrar Registration Expiration Date: 2025-06-26T16:33:04Z Registrar: Hostinger Operations, UAB Registrar IANA ID: 1636 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: 10 Corporate Drive Registrant City: Burlington Registrant State/Province: MA Registrant Postal Code: 01803 Registrant Country: US Registrant Phone: +1.8022274003 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@privacyprotect.org Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: Privacy Protect, LLC (PrivacyProtect.org) Admin Street: 10 Corporate Drive Admin City: Burlington Admin State/Province: MA Admin Postal Code: 01803 Admin Country: US Admin Phone: +1.8022274003

	Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact@privacyprotect.org Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: Privacy Protect, LLC (PrivacyProtect.org) Tech Street: 10 Corporate Drive Tech City: Burlington Tech State/Province: MA Tech Postal Code: 01803 Tech Country: US Tech Phone: +1.8022274003 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@privacyprotect.org Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse@hostinger.com Registrar Abuse Contact Phone: +37064503378 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-20T17:59:47Z <<<
MURODJONOVS.COM	Domain Name: MURODJONOVS.COM Registry Domain ID: 2890773051_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.hostinger.com Registrar URL: https://www.hostinger.com Updated Date: 2024-08-15T02:17:11Z Creation Date: 2024-06-15T16:27:23Z Registrar Registration Expiration Date: 2025-06-15T16:27:23Z Registrar: Hostinger Operations, UAB Registrar IANA ID: 1636 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: 10 Corporate Drive Registrant City: Burlington

	Registrant State/Province: MA Registrant Postal Code: 01803 Registrant Country: US Registrant Phone: +1.8022274003 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@privacyprotect.org Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: Privacy Protect, LLC (PrivacyProtect.org) Admin Street: 10 Corporate Drive Admin City: Burlington Admin State/Province: MA Admin Postal Code: 01803 Admin Country: US Admin Phone: +1.8022274003 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact@privacyprotect.org Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: Privacy Protect, LLC (PrivacyProtect.org) Tech Street: 10 Corporate Drive Tech City: Burlington Tech State/Province: MA Tech Postal Code: 01803 Tech Country: US Tech Phone: +1.8022274003 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@privacyprotect.org Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse@hostinger.com Registrar Abuse Contact Phone: +37064503378 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
OSOMTOYS.COM	Domain Name: OSOMTOYS.COM Registry Domain ID: 2774429345_DOMAIN_COM-VRSN

	Registrar WHOIS Server: whois.ownregistrar.com Registrar URL: http://www.ownregistrar.com Updated Date: 2024-04-21T07:07:45Z Creation Date: 2023-04-20T08:04:32Z Registry Expiry Date: 2025-04-20T08:04:32Z Registrar: OwnRegistrar, Inc. Registrar IANA ID: 1250 Registrar Abuse Contact Email: Registrar Abuse Contact Phone: Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: NS1.CR25.MANAGEDNS.ORG Name Server: NS2.CR25.MANAGEDNS.ORG DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
OWAORGANIZESPACE.COM	Domain name: owaorganizespace.com Registry Domain ID: 2750404096_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-01-10T15:33:26.00Z Registrar Registration Expiration Date: 2024-01-10T15:33:26.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext:

	Registrant Email: fbf088d1456b4705bf347ad8cd8af164.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: fbf088d1456b4705bf347ad8cd8af164.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: fbf088d1456b4705bf347ad8cd8af164.protect@withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ For more information on Whois status codes, please visit https://icann.org/epp
POSTREQUESTIN.COM	Domain name: postrequestin.com Registry Domain ID: 2805036855_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com

	Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-08-11T13:13:23.00Z Registrar Registration Expiration Date: 2024-08-11T13:13:23.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: REACTIVATION PERIOD Registrant Organization: Withheld for Privacy Purposes Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: reactivation-pending@mail.withheldforprivacy.com Registry Admin ID: Admin Name: REACTIVATION PERIOD Admin Organization: Withheld for Privacy Purposes Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: reactivation-pending@mail.withheldforprivacy.com Registry Tech ID: Tech Name: REACTIVATION PERIOD Tech Organization: Withheld for Privacy Purposes Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region

	Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: reactivation-pending@mail.withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
PROFFSOLUTION.COM	Domain name: proffsolution.com Registry Domain ID: 2781360245_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-05-16T14:20:42.00Z Registrar Registration Expiration Date: 2024-05-16T14:20:42.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: d3d1189d859748a39e4705e5c3eb7563.protect@withheldforprivacy.com Registry Admin ID:

	Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: d3d1189d859748a39e4705e5c3eb7563.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: d3d1189d859748a39e4705e5c3eb7563.protect@withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ For more information on Whois status codes, please visit https://icann.org/epp
PROTECTORDOCUMENTCENTER.COM	Domain name: protectordocumentcenter.com Registry Domain ID: 2765526395_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-03-16T09:09:27.00Z

	Registrar Registration Expiration Date: 2024-03-16T09:09:27.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: b1b68209f55246fdbce545ee00e76782.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: b1b68209f55246fdbce545ee00e76782.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2

	Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: b1b68209f55246fdbce545ee00e76782.protect@withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ For more information on Whois status codes, please visit https://icann.org/epp
PUREAFRO.COM	Domain Name: PUREAFRO.COM Registry Domain ID: 1544497306_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.tucows.com Registrar URL: http://www.tucows.com Updated Date: 2024-09-02T16:38:02Z Creation Date: 2009-02-27T09:26:23Z Registry Expiry Date: 2025-02-27T09:26:23Z Registrar: Tucows Domains Inc. Registrar IANA ID: 69 Registrar Abuse Contact Email: domainabuse@tucows.com Registrar Abuse Contact Phone: +1.4165350123 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: GAIL.NS.CLOUDFLARE.COM Name Server: NORMAN.NS.CLOUDFLARE.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2024-09-20T19:29:28Z <<<
RISEUPBIT.COM	Domain name: riseupbit.com Registry Domain ID: 2837954116_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com

	Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-12-15T17:32:12.00Z Registrar Registration Expiration Date: 2024-12-15T17:32:12.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: f193dbb5779c4ab995104643badb8655.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: f193dbb5779c4ab995104643badb8655.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy

	Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: f193dbb5779c4ab995104643badb8655.protect@withheldforprivacy.com Name Server: ns1.timeweb.ru Name Server: ns2.timeweb.ru Name Server: ns3.timeweb.org Name Server: ns4.timeweb.org DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-20T15:30:42.89Z <<<
SECLAWDOORWAY.COM	Domain name: SECLAWDOORWAY.COM Registry Domain ID: 2798235248_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-07-14T15:28:39.00Z Registrar Registration Expiration Date: 2024-07-14T15:28:39.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: pendingDelete https://icann.org/epp#pendingDelete Domain Status: redemptionPeriod https://icann.org/epp#redemptionPeriod Registry Registrant ID: Registrant Name: REACTIVATION PERIOD Registrant Organization: Withheld for Privacy Purposes

	Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: reactivation-pending@mail.withheldforprivacy.com Registry Admin ID: Admin Name: REACTIVATION PERIOD Admin Organization: Withheld for Privacy Purposes Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: reactivation-pending@mail.withheldforprivacy.com Registry Tech ID: Tech Name: REACTIVATION PERIOD Tech Organization: Withheld for Privacy Purposes Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: reactivation-pending@mail.withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-19T22:32:36.22Z <<<

SETUPPROFI.COM	Domain name: setupprofi.com Registry Domain ID: 2780256398_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-05-12T15:35:52.00Z Registrar Registration Expiration Date: 2024-05-12T15:35:52.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 309d713534bb4d579cb3d520a42b69fa.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext:

	Admin Email: 309d713534bb4d579cb3d520a42b69fa.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 309d713534bb4d579cb3d520a42b69fa.protect@withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ For more information on Whois status codes, please visit https://icann.org/epp
SKELETCHECK.COM	Domain Name: SKELETCHECK.COM Registry Domain ID: 2863745777_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.hostinger.com Registrar URL: https://www.hostinger.com Updated Date: 2024-05-15T02:16:44Z Creation Date: 2024-03-15T12:17:37Z Registrar Registration Expiration Date: 2025-03-15T12:17:37Z Registrar: Hostinger Operations, UAB Registrar IANA ID: 1636 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: 10 Corporate Drive Registrant City: Burlington Registrant State/Province: MA

	Registrant Postal Code: 01803 Registrant Country: US Registrant Phone: +1.8022274003 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@privacyprotect.org Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: Privacy Protect, LLC (PrivacyProtect.org) Admin Street: 10 Corporate Drive Admin City: Burlington Admin State/Province: MA Admin Postal Code: 01803 Admin Country: US Admin Phone: +1.8022274003 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact@privacyprotect.org Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: Privacy Protect, LLC (PrivacyProtect.org) Tech Street: 10 Corporate Drive Tech City: Burlington Tech State/Province: MA Tech Postal Code: 01803 Tech Country: US Tech Phone: +1.8022274003 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@privacyprotect.org Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse@hostinger.com Registrar Abuse Contact Phone: +37064503378 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-20T19:35:08Z <<<
SKYINFORMDATA.COM	Domain name: skyinformdata.com

	Registry Domain ID: 2779936825_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2024-06-11T01:51:10.59Z Creation Date: 2023-05-11T11:10:35.00Z Registrar Registration Expiration Date: 2025-05-11T11:10:35.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 1416e66ba6314846af7dc61b5becfb23.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext:

	Admin Email: 1416e66ba6314846af7dc61b5becfb23.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 1416e66ba6314846af7dc61b5becfb23.protect@withheldforprivacy.com Name Server: ns1.dan.com Name Server: ns2.dan.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-19T21:35:49.33Z <<<
STORAGEINFORMATIONSOLUTIONS.COM	Domain name: storageinformationsolutions.com Registry Domain ID: 2775716410_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-04-25T15:33:03.00Z Registrar Registration Expiration Date: 2024-04-25T15:33:03.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf

	Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 849a9c20eedf4ba6917e5e3b004b51f0.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 849a9c20eedf4ba6917e5e3b004b51f0.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 849a9c20eedf4ba6917e5e3b004b51f0.protect@withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com

	DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ For more information on Whois status codes, please visit https://icann.org/epp
TARIFJANE.COM	Domain Name: TARIFJANE.COM Registry Domain ID: 2806534838_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2024-08-18T07:19:27Z Creation Date: 2023-08-17T14:05:41Z Registry Expiry Date: 2025-08-17T14:05:41Z Registrar: NameCheap, Inc. Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: DNS101.REGISTRAR-SERVERS.COM Name Server: DNS102.REGISTRAR-SERVERS.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2024-09-20T19:37:47Z <<<
TRANSLATESPLIT.COM	Domain Name: TRANSLATESPLIT.COM Registry Domain ID: 2804793747_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2024-08-11T07:26:26Z Creation Date: 2023-08-10T16:47:53Z Registry Expiry Date: 2025-08-10T16:47:53Z Registrar: NameCheap, Inc. Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: DNS101.REGISTRAR-SERVERS.COM Name Server: DNS102.REGISTRAR-SERVERS.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

	>>> Last update of whois database: 2024-09-20T19:42:00Z <<<
VOCABPAPER.COM	Domain Name: VOCABPAPER.COM Registry Domain ID: 2863768341_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.hostinger.com Registrar URL: http://www.hostinger.com Updated Date: 2024-03-15T15:54:19Z Creation Date: 2024-03-15T15:54:15Z Registry Expiry Date: 2025-03-15T15:54:15Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636 Registrar Abuse Contact Email: abuse-tracker@hostinger.com Registrar Abuse Contact Phone: +37064503378 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: NS1.DNS-PARKING.COM Name Server: NS2.DNS-PARKING.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2024-09-20T19:43:45Z <<<
VOLTCLOUDPINE.COM	Domain Name: VOLTCLOUDPINE.COM Registry Domain ID: 2859317801_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2024-02-28T18:56:11Z Creation Date: 2024-02-28T18:35:17Z Registry Expiry Date: 2025-02-28T18:35:17Z Registrar: NameCheap, Inc. Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: NS1.DNS-PARKING.COM Name Server: NS2.DNS-PARKING.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2024-09-20T19:45:32Z <<<

WARDENGOVERMENTLAW.COM	Domain Name: WARDENGOVERMENTLAW.COM Registry Domain ID: 2798235251_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2024-08-25T15:39:46Z Creation Date: 2023-07-14T15:28:43Z Registry Expiry Date: 2024-07-14T15:28:43Z Registrar: NameCheap, Inc. Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: redemptionPeriod https://icann.org/epp#redemptionPeriod Name Server: DNS101.REGISTRAR-SERVERS.COM Name Server: DNS102.REGISTRAR-SERVERS.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2024-09-20T19:47:01Z <<<
WEBFIGMADESIGNERSHOP.COM	Domain name: WEBFIGMADESIGNERSHOP.COM Registry Domain ID: 2801604572_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-07-28T16:09:07.00Z Registrar Registration Expiration Date: 2024-07-28T16:09:07.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: pendingDelete https://icann.org/epp#pendingDelete Domain Status: redemptionPeriod https://icann.org/epp#redemptionPeriod Registry Registrant ID: Registrant Name: REACTIVATION PERIOD Registrant Organization: Withheld for Privacy Purposes

	Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: reactivation-pending@mail.withheldforprivacy.com Registry Admin ID: Admin Name: REACTIVATION PERIOD Admin Organization: Withheld for Privacy Purposes Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: reactivation-pending@mail.withheldforprivacy.com Registry Tech ID: Tech Name: REACTIVATION PERIOD Tech Organization: Withheld for Privacy Purposes Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: reactivation-pending@mail.withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-20T06:53:23.21Z <<<

WEBITRESOURSE.COM	Domain name: webitresourse.com Registry Domain ID: 2786631354_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-06-02T19:35:46.00Z Registrar Registration Expiration Date: 2024-06-02T19:35:46.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 042db3c6b292404b9120c05a47705b42.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext:

	Admin Email: 042db3c6b292404b9120c05a47705b42.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 042db3c6b292404b9120c05a47705b42.protect@withheldforprivacy.com Name Server: dns101.registrar-servers.com Name Server: dns102.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ For more information on Whois status codes, please visit https://icann.org/epp
XACSHOP.COM	Domain Name: XACSHOP.COM Registry Domain ID: 2870474432_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.hostinger.com Registrar URL: http://www.hostinger.com Updated Date: 2024-04-08T13:50:55Z Creation Date: 2024-04-08T13:50:51Z Registry Expiry Date: 2025-04-08T13:50:51Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636 Registrar Abuse Contact Email: abuse-tracker@hostinger.com Registrar Abuse Contact Phone: +37064503378 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: NS1.DNS-PARKING.COM Name Server: NS2.DNS-PARKING.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

	>>> Last update of whois database: 2024-09-20T19:54:05Z <<<

.ORG REGISTRY
Public Interest Registry
11911 Freedom Drive, 10th Floor, Suite 1000
Reston, VA 20190

.ORG DOMAINS

EDITABLEZOOM.ORG	Domain Name: editablezoom.org Registry Domain ID: 40b4413522e74dc1ae89007355f64092-LROR Registrar WHOIS Server: https://rdapserver.net/ Registrar URL: http://www.hostinger.com Updated Date: 2024-03-20T13:34:36Z Creation Date: 2024-03-15T13:33:57Z Registry Expiry Date: 2025-03-15T13:33:57Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636 Registrar Abuse Contact Email: Registrar Abuse Contact Phone: Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: MA Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY

	Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of WHOIS database: 2024-09-20T19:56:16Z <<<
EICHENFASS.ORG	Domain Name: eichenfass.org Registry Domain ID: ecfc396b7971434c9970a1cdf34568ad-LROR Registrar WHOIS Server: https://rdapserver.net/ Registrar URL: http://www.hostinger.com Updated Date: 2024-07-13T16:19:35Z Creation Date: 2024-07-08T16:18:37Z Registry Expiry Date: 2025-07-08T16:18:37Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636 Registrar Abuse Contact Email: Registrar Abuse Contact Phone:

	Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: MA Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY

	Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of WHOIS database: 2024-09-20T19:56:51Z <<<
GOTHICSHOP.ORG	Domain Name: gothicshop.org Registry Domain ID: 29102a533cb94a9fb8c9dd5f9bd122e4-LROR Registrar WHOIS Server: https://rdapserver.net/ Registrar URL: http://www.hostinger.com Updated Date: 2024-05-12T13:14:54Z Creation Date: 2024-05-07T13:14:35Z Registry Expiry Date: 2025-05-07T13:14:35Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636 Registrar Abuse Contact Email: Registrar Abuse Contact Phone: Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: MA Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.

	Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of WHOIS database: 2024-09-20T19:57:35Z <<<
INVESTFIX.ORG	Domain Name: investfix.org Registry Domain ID: b2bfa484594b41ec91cd184c753d301d-LROR Registrar WHOIS Server: https://rdapserver.net/ Registrar URL: http://www.hostinger.com Updated Date: 2024-07-08T15:37:05Z Creation Date: 2024-07-03T15:36:27Z

	Registry Expiry Date: 2025-07-03T15:36:27Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636 Registrar Abuse Contact Email: Registrar Abuse Contact Phone: Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: MA Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY

	Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of WHOIS database: 2024-09-20T19:57:58Z <<<
LOYALTYFIRST.ORG	Domain Name: loyaltyfirst.org Registry Domain ID: 41b01ee0b0f44d80ac8c5eb249f3d7d6-LROR Registrar WHOIS Server: https://rdapserver.net/ Registrar URL: http://www.hostinger.com Updated Date: 2024-07-10T18:03:19Z Creation Date: 2024-07-05T18:02:58Z Registry Expiry Date: 2025-07-05T18:02:58Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636 Registrar Abuse Contact Email: Registrar Abuse Contact Phone: Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: MA Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY

	Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
MTGCGROUP.ORG	Domain Name: mtgcgroup.org

	Registry Domain ID: a0836b7399a443a58ef7b37113462d42-LROR Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2024-03-11T16:26:58Z Creation Date: 2024-03-06T16:26:32Z Registry Expiry Date: 2025-03-06T16:26:32Z Registrar: NameCheap, Inc. Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: Capital Region Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: IS Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.

	Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of WHOIS database: 2024-09-20T19:59:11Z <<<
MUTUALRESCUEBOOK.ORG	Domain Name: mutualrescuebook.org Registry Domain ID: ec34753585114c108fc4a7235a77ad00-LROR Registrar WHOIS Server: https://rdapserver.net/ Registrar URL: http://www.hostinger.com Updated Date: 2024-07-12T16:08:34Z Creation Date: 2024-05-19T12:01:07Z Registry Expiry Date: 2025-05-19T12:01:07Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636 Registrar Abuse Contact Email: Registrar Abuse Contact Phone: Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: MA Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US

	Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

	>>> Last update of WHOIS database: 2024-09-20T20:00:45Z <<<
MYGEIGER.ORG	Domain Name: mygeiger.org Registry Domain ID: b160a2dbb15a4f2bac6d38412760c675-LROR Registrar WHOIS Server: https://rdapserver.net/ Registrar URL: http://www.hostinger.com Updated Date: 2024-04-24T15:53:16Z Creation Date: 2024-04-19T15:53:10Z Registry Expiry Date: 2025-04-19T15:53:10Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636 Registrar Abuse Contact Email: Registrar Abuse Contact Phone: Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: MA Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY

	Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of WHOIS database: 2024-09-20T20:01:18Z <<<
PARTICLESOLID.ORG	Domain Name: particlesolid.org Registry Domain ID: c3e9dad867f74507b8bfd5e435089a6f-LROR Registrar WHOIS Server: https://rdapserver.net/ Registrar URL: http://www.hostinger.com Updated Date: 2024-04-29T09:48:58Z Creation Date: 2024-03-01T18:09:00Z Registry Expiry Date: 2025-03-01T18:09:00Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636 Registrar Abuse Contact Email: Registrar Abuse Contact Phone: Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: REDACTED FOR PRIVACY

	Registrant City: REDACTED FOR PRIVACY Registrant State/Province: MA Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: 123ns1.dns-parking.com Name Server: 123ns2.dns-parking.com

	DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of WHOIS database: 2024-09-20T20:02:01Z <<<
QUANTUMNYX.ORG	Domain Name: quantumnyx.org Registry Domain ID: 408f350f60f44bb6bc5fe23ba8878f84-LROR Registrar WHOIS Server: https://rdapserver.net/ Registrar URL: http://www.hostinger.com Updated Date: 2024-07-24T16:12:48Z Creation Date: 2024-07-19T16:12:16Z Registry Expiry Date: 2025-07-19T16:12:16Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636 Registrar Abuse Contact Email: Registrar Abuse Contact Phone: Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: MA Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY

	Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of WHOIS database: 2024-09-20T20:02:42Z <<<
YAMARU.ORG	Domain Name: yamaru.org Registry Domain ID: 208695d5b71e497d9409d71ae3409fc7-LROR Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2024-03-11T15:28:19Z Creation Date: 2024-03-06T15:27:54Z Registry Expiry Date: 2025-03-06T15:27:54Z Registrar: NameCheap, Inc. Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY

	Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: Capital Region Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: IS Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for

	information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of WHOIS database: 2024-09-20T20:03:34Z <<<

.NET REGISTRY
VeriSign Global Registry Services
12061 Bluemont Way
Reston VA 20190

.NET DOMAIN

DESGNSPIRATION.NET	Domain Name: DESGNSPIRATION.NET Registry Domain ID: 2862669470_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.PublicDomainRegistry.com Registrar URL: http://www.publicdomainregistry.com Updated Date: 2024-03-11T13:16:14Z Creation Date: 2024-03-11T13:16:14Z Registry Expiry Date: 2025-03-11T13:16:14Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Registrar Abuse Contact Email: Registrar Abuse Contact Phone: +1.2013775952 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: DNS1.REGWAY.COM Name Server: DNS2.REGWAY.COM Name Server: DNS3.REGWAY.COM Name Server: DNS4.REGWAY.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2024-09-20T20:08:43Z <<<
JUSTAPPLE.NET	Domain Name: justapple.net Registry Domain ID: 2867801843_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2024-03-29T15:49:10Z Creation Date: 2024-03-29T15:49:07Z Registry Expiry Date: 2025-03-29T15:49:07Z Registrar: NameCheap, Inc. Registrar IANA ID: 1068

	Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: DNS1.REGISTRAR-SERVERS.COM Name Server: DNS2.REGISTRAR-SERVERS.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2024-09-20T20:10:42Z <<<
OMMAHAT.NET	Domain name: ommahat.net Registry Domain ID: 2864908040_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2024-03-19T12:16:58.00Z Registrar Registration Expiration Date: 2025-03-19T12:16:58.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 2047e9ea4c3f42bab22af7c54e1a5295.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2

	Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 2047e9ea4c3f42bab22af7c54e1a5295.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 2047e9ea4c3f42bab22af7c54e1a5295.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-20T14:12:19.77Z <<<
CITYESSENTIALS.NET	Domain Name: CITYESSENTIALS.NET Registry Domain ID: 2882624142_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.hostinger.com Registrar URL: https://www.hostinger.com Updated Date: 2024-07-19T02:16:49Z Creation Date: 2024-05-19T15:30:15Z Registrar Registration Expiration Date: 2025-05-19T15:30:15Z Registrar: Hostinger Operations, UAB Registrar IANA ID: 1636 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry

	Registrant Name: Domain Admin Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: 10 Corporate Drive Registrant City: Burlington Registrant State/Province: MA Registrant Postal Code: 01803 Registrant Country: US Registrant Phone: +1.8022274003 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@privacyprotect.org Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: Privacy Protect, LLC (PrivacyProtect.org) Admin Street: 10 Corporate Drive Admin City: Burlington Admin State/Province: MA Admin Postal Code: 01803 Admin Country: US Admin Phone: +1.8022274003 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact@privacyprotect.org Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: Privacy Protect, LLC (PrivacyProtect.org) Tech Street: 10 Corporate Drive Tech City: Burlington Tech State/Province: MA Tech Postal Code: 01803 Tech Country: US Tech Phone: +1.8022274003 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@privacyprotect.org Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse@hostinger.com Registrar Abuse Contact Phone: +37064503378 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-20T20:13:44Z <<<

SGMODS.NET	Domain name: sgmods.net Registry Domain ID: 2875558934_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2024-04-25T14:39:04.00Z Registrar Registration Expiration Date: 2025-04-25T14:39:04.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: b8999297390441729eddc3a8cc2bf368.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext:

	Admin Email: b8999297390441729eddc3a8cc2bf368.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: b8999297390441729eddc3a8cc2bf368.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-09-20T19:15:52.11Z <<<

.ONLINE REGISTRY
Radix Technologies Inc.
Services Cayman Limited, P.O. Box 10008, Willow House, Cricket Square, Grand Cayman KY1-1001
Cayman Islands (the)

.ONLINE DOMAIN

PROTECTIONOFFICE.ONLINE	Domain Name: PROTECTIONOFFICE.ONLINE Registry Domain ID: D319531822-CNIC Registrar WHOIS Server: whois.hostinger.com Registrar URL: https://www.hostinger.com/ Updated Date: 2023-08-26T01:06:09.0Z Creation Date: 2022-08-25T07:55:24.0Z Registry Expiry Date: 2024-08-25T23:59:59.0Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

	Domain Status: autoRenewPeriod https://icann.org/epp#autoRenewPeriod Registrant Organization: Not Applicable Registrant State/Province: FL Registrant Country: US Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: DNS3.PARKPAGE.FOUNDATIONAPI.COM Name Server: DNS4.PARKPAGE.FOUNDATIONAPI.COM DNSSEC: unsigned Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registrar Abuse Contact Email: domains@hostinger.com Registrar Abuse Contact Phone: +370.68424669 URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

.TECH REGISTRY
Radix Technologies Inc.
Services Cayman Limited, P.O. Box 10008, Willow House, Cricket Square, Grand Cayman KY1-1001
Cayman Islands (the)

.TECH DOMAIN

PREVIEW-DOCUMENT.TECH	Domain Name: PREVIEW-DOCUMENT.TECH Registry Domain ID: D361616076-CNIC Registrar WHOIS Server: whois.hostinger.com Registrar URL: https://www.hostinger.com/ Updated Date: 2024-05-21T01:36:58.0Z Creation Date: 2023-04-14T12:54:16.0Z Registry Expiry Date: 2024-04-14T23:59:59.0Z Registrar: HOSTINGER operations, UAB

	Registrar IANA ID: 1636 Domain Status: pendingDelete https://icann.org/epp#pendingDelete Domain Status: serverHold https://icann.org/epp#serverHold Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: redemptionPeriod https://icann.org/epp#redemptionPeriod Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant State/Province: MA Registrant Country: US Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: NS1.DNS-EXPIRED.COM Name Server: NS2.DNS-EXPIRED.COM DNSSEC: unsigned Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registrar Abuse Contact Email: abuse@hostinger.com Registrar Abuse Contact Phone: +370.68424669 URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
PROTECTIONOFFICE.TECH	Domain Name: PROTECTIONOFFICE.TECH Registry Domain ID: D401427312-CNIC Registrar WHOIS Server: whois.hostinger.com Registrar URL: https://www.hostinger.com/ Updated Date: 2023-10-10T11:34:53.0Z Creation Date: 2023-10-05T11:33:46.0Z Registry Expiry Date: 2024-10-05T23:59:59.0Z Registrar: HOSTINGER operations, UAB Registrar IANA ID: 1636

	Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant State/Province: MA Registrant Country: US Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: NS2.PROTECTIONOFFICE.TECH Name Server: NS1.PROTECTIONOFFICE.TECH DNSSEC: unsigned Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registrar Abuse Contact Email: abuse@hostinger.com Registrar Abuse Contact Phone: +370.68424669 URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of WHOIS database: 2024-09-20T20:22:04.0Z <<<

APPENDIX B

United States of America
United States Patent and Trademark Office

MICROSOFT

Reg. No. 6,880,851

Registered Oct. 18, 2022

Int. Cl.: 35

Service Mark

Principal Register

Microsoft Corporation (WASHINGTON CORPORATION)
One Microsoft Way
Redmond, WASHINGTON 98052

CLASS 35: Business services, namely, business consultation services, business advice and information services; business marketing services; business consulting services; business networking; providing information in the fields of business and commerce over global computer networks and global communications networks; providing consumer product information via the Internet; providing office functions; retail store and online retail store services featuring a wide variety of consumer goods of others; retail store services in the field of office products; online retail store services featuring computers, computer hardware, computer peripherals, laptops, tablets, portable music players, personal digital assistants, cell phones, digital media streaming devices, computer software, applications for personal computers, video game consoles, video game controllers, video games, gaming software, gaming equipment, security services, downloadable movies and television shows, webcams, books, clothing, back packs, messenger bags, computer bags, notebooks, journals, laptop sleeves, stickers, pens, pencils, toys, gift cards and novelty items; operating online marketplaces featuring software applications; provision of an on-line marketplace for buyers and sellers of goods and services; operating on-line marketplaces for sellers and buyers of goods and/or services; providing retail store and prepaid subscription services featuring downloadable, pre-recorded text, data, image, audio, video, and multimedia files, provided via the internet and other electronic and communications networks; compiling of information into computer databases, namely, compiling of internet based information and providing such information in response to voice or text controlled inquiries; advertising services; advertising and directory services, namely, promoting the services of others by providing a web page featuring links to the websites of others; digital advertising services; online advertising on a computer network; providing websites and applications featuring business related news and information; providing an internet website featuring news and information in the field of national and international politics; organization and conducting of virtual commercial exhibitions in the field of computers, artificial intelligence, information technology, and electronic business transactions via a global computer network; charitable services, namely, organizing, developing, and conducting volunteer and not-for-profit programs and volunteer and not-for-profit projects aimed at increasing technological development in rural and underdeveloped communities; organizing and developing charitable projects that aim to promote the importance of reading, writing, science, technology, engineering and math;

Katherine Kelly Vidal

Director of the United States
Patent and Trademark Office

promoting public awareness of and the need to support social and economic development; charitable services, namely, organizing and conducting volunteer programs, community service projects and neighborhood improvement projects; information, advice and consultancy regarding the aforementioned services; organizing, promoting and conducting online, business-to-business events and webinars in the field of computing and digital transformation; organizing, arranging, conducting and promoting of trade shows, business, commercial, and promotional exhibitions and business conferences in the fields of computer hardware, software, telecommunications, and high technology and in the field of development of computer programs and systems; charitable services, namely, organizing and conducting volunteer programs to build and grow sustainable computer science programs through partnerships between classroom teachers and technology industry volunteers in the fields of technology education and literacy in schools; business management and advisory services in the agriculture field; business consulting services in the agriculture field; provision of business information relating to agricultural industry via global computer networks; business analysis, research and information services in the agriculture field; business services, namely, compilation and collection of data, information and statistics, business management data and data relating to the administration of farms and agricultural projects using technologies that include the internet of things (IoT), blockchain, robotics, software as a service (SaaS), platforms as a service (PaaS) and artificial intelligence; business management and advertising services for others, namely, assisting others in direct electronic mail advertising, assisting others in placing and running advertisements on computer networks and global communications networks; business on-line information services, namely, providing databases and website links to other content providers in the field of business issues; Promoting, marketing and advertising the brands and goods of others related to the computer software, applications, computer and video games and audio visual content sale and retail services industries; online retail store services in the field of computer software, applications, computer and video games and audio visual content; business data analysis services in the field of computers, artificial intelligence, information technology, and electronic business transactions via a global computer network; analyzing and compiling business data; market analysis and research services relating to customer behavior, satisfaction, attitude, effectiveness; computerized database management; marketing data integration; data processing services; market research and market analysis services; statistical analysis and compilation for business purposes; economic forecasting; market research and business analysis; preparation of business marketing information from and into computer database form; Marketing services, namely, preparation of product and company literature for others; online service for connecting social network users with retailers for the purpose of facilitating discounted purchases; compilation of information into computer databases; compilation of statistics for commercial purposes; compilation and systemization of information into computer databases; compilation of advertisements for use as web pages on the Internet; advertising on the Internet for others; distribution of advertising materials; Internet advertising services; advertising analysis; advertising and promotional services; advertising and marketing services; pay per click advertising; developing and coordinating volunteer projects for charitable organizations; providing business information via a website; providing a searchable on-line advertising website and guide featuring the goods and services of other vendors via the Internet; online advertising network matching services for connecting advertisers to websites; providing career information; arranging and conducting special events for business purposes; promotion of goods and services through sponsorship of sports events; arranging subscriptions to video games, computer games, and game content, for others; advisory and consultancy services relating to all the aforesaid services

FIRST USE 11-12-1975; IN COMMERCE 11-12-1975

THE MARK CONSISTS OF STANDARD CHARACTERS WITHOUT CLAIM TO ANY PARTICULAR FONT STYLE, SIZE OR COLOR

SER. NO. 90-402,126, FILED 12-22-2020

REQUIREMENTS TO MAINTAIN YOUR FEDERAL TRADEMARK REGISTRATION

WARNING: YOUR REGISTRATION WILL BE CANCELLED IF YOU DO NOT FILE THE DOCUMENTS BELOW DURING THE SPECIFIED TIME PERIODS.

Requirements in the First Ten Years*
What and When to File:

- ***First Filing Deadline:*** You must file a Declaration of Use (or Excusable Nonuse) between the 5th and 6th years after the registration date. See 15 U.S.C. §§1058, 1141k. If the declaration is accepted, the registration will continue in force for the remainder of the ten-year period, calculated from the registration date, unless cancelled by an order of the Commissioner for Trademarks or a federal court.

- ***Second Filing Deadline:*** You must file a Declaration of Use (or Excusable Nonuse) and an Application for Renewal between the 9th and 10th years after the registration date.* See 15 U.S.C. §1059.

Requirements in Successive Ten-Year Periods*
What and When to File:

- You must file a Declaration of Use (or Excusable Nonuse) and an Application for Renewal between every 9th and 10th-year period, calculated from the registration date.*

Grace Period Filings*

The above documents will be accepted as timely if filed within six months after the deadlines listed above with the payment of an additional fee.

***ATTENTION MADRID PROTOCOL REGISTRANTS:** The holder of an international registration with an extension of protection to the United States under the Madrid Protocol must timely file the Declarations of Use (or Excusable Nonuse) referenced above directly with the United States Patent and Trademark Office (USPTO). The time periods for filing are based on the U.S. registration date (not the international registration date). The deadlines and grace periods for the Declarations of Use (or Excusable Nonuse) are identical to those for nationally issued registrations. See 15 U.S.C. §§1058, 1141k. However, owners of international registrations do not file renewal applications at the USPTO. Instead, the holder must file a renewal of the underlying international registration at the International Bureau of the World Intellectual Property Organization, under Article 7 of the Madrid Protocol, before the expiration of each ten-year term of protection, calculated from the date of the international registration. See 15 U.S.C. §1141j. For more information and renewal forms for the international registration, see http://www.wipo.int/madrid/en/.

NOTE: Fees and requirements for maintaining registrations are subject to change. Please check the USPTO website for further information. With the exception of renewal applications for registered extensions of protection, you can file the registration maintenance documents referenced above online at http://www.uspto.gov.

NOTE: A courtesy e-mail reminder of USPTO maintenance filing deadlines will be sent to trademark owners/holders who authorize e-mail communication and maintain a current e-mail address with the USPTO. To ensure that e-mail is authorized and your address is current, please use the Trademark Electronic Application System (TEAS) Correspondence Address and Change of Owner Address Forms available at http://www.uspto.gov.

United States of America
United States Patent and Trademark Office

OUTLOOK

Reg. No. 4,255,129

Registered Dec. 4, 2012

Int. Cl.: 42

SERVICE MARK

PRINCIPAL REGISTER

MICROSOFT CORPORATION (WASHINGTON CORPORATION)
ONE MICROSOFT WAY
REDMOND, WA 980526399

FOR: CLOUD COMPUTING FEATURING SOFTWARE FOR USE IN EMAIL, CALENDARING, CONTACTS MANAGEMENT AND ACCESSING REMOTELY STORED DATA FOR SUCH APPLICATIONS; PROVIDING TEMPORARY USE OF ON-LINE NON-DOWNLOADABLE SOFTWARE AND APPLICATIONS FOR EMAIL, CALENDARING, AND CONTACTS MANAGEMENT; PROVIDING TECHNICAL INFORMATION IN THE FIELD OF COMPUTER SOFTWARE AND CLOUD COMPUTING, IN CLASS 42 (U.S. CLS. 100 AND 101).

FIRST USE 3-2-2008; IN COMMERCE 3-2-2008.

THE MARK CONSISTS OF STANDARD CHARACTERS WITHOUT CLAIM TO ANY PARTICULAR FONT, STYLE, SIZE, OR COLOR.

OWNER OF U.S. REG. NO. 2,188,125.

SN 85-467,641, FILED 11-8-2011.

SETH A. RAPPAPORT, EXAMINING ATTORNEY

David J. Kappos

Director of the United States Patent and Trademark Office

REQUIREMENTS TO MAINTAIN YOUR FEDERAL TRADEMARK REGISTRATION

WARNING: YOUR REGISTRATION WILL BE CANCELLED IF YOU DO NOT FILE THE DOCUMENTS BELOW DURING THE SPECIFIED TIME PERIODS.

Requirements in the First Ten Years*
What and When to File:

First Filing Deadline: You must file a Declaration of Use (or Excusable Nonuse) between the 5th and 6th years after the registration date. *See* 15 U.S.C. §§1058, 1141k. If the declaration is accepted, the registration will continue in force for the remainder of the ten-year period, calculated from the registration date, unless cancelled by an order of the Commissioner for Trademarks or a federal court.

Second Filing Deadline: You must file a Declaration of Use (or Excusable Nonuse) **and** an Application for Renewal between the 9th and 10th years after the registration date.* *See* 15 U.S.C. §1059.

Requirements in Successive Ten-Year Periods*
What and When to File:

You must file a Declaration of Use (or Excusable Nonuse) **and** an Application for Renewal between every 9th and 10th-year period, calculated from the registration date.*

Grace Period Filings*

The above documents will be accepted as timely if filed within six months after the deadlines listed above with the payment of an additional fee.

The United States Patent and Trademark Office (USPTO) will NOT send you any future notice or reminder of these filing requirements.

***ATTENTION MADRID PROTOCOL REGISTRANTS:** The holder of an international registration with an extension of protection to the United States under the Madrid Protocol must timely file the Declarations of Use (or Excusable Nonuse) referenced above directly with the USPTO. The time periods for filing are based on the U.S. registration date (not the international registration date). The deadlines and grace periods for the Declarations of Use (or Excusable Nonuse) are identical to those for nationally issued registrations. *See* 15 U.S.C. §§1058, 1141k. However, owners of international registrations do not file renewal applications at the USPTO. Instead, the holder must file a renewal of the underlying international registration at the International Bureau of the World Intellectual Property Organization, under Article 7 of the Madrid Protocol, before the expiration of each ten-year term of protection, calculated from the date of the international registration. *See* 15 U.S.C. §1141j. For more information and renewal forms for the international registration, see http://www.wipo.int/madrid/en/.

NOTE: Fees and requirements for maintaining registrations are subject to change. Please check the USPTO website for further information. With the exception of renewal applications for registered extensions of protection, you can file the registration maintenance documents referenced above online at http://www.uspto.gov.

United States of America
United States Patent and Trademark Office

ONEDRIVE

Reg. No. 4,661,770

Registered Dec. 30, 2014

Int. Cls.: 9, 38, 39 and 42

TRADEMARK

SERVICE MARK

PRINCIPAL REGISTER

MICROSOFT CORPORATION (WASHINGTON CORPORATION)
ONE MICROSOFT WAY
REDMOND, WA 980526399

FOR: COMPUTER SOFTWARE FOR USE IN ELECTRONIC STORAGE OF DATA FEATURING CLOUD COMPUTING , IN CLASS 9 (U.S. CLS. 21, 23, 26, 36 AND 38).

FIRST USE 2-19-2014; IN COMMERCE 2-19-2014.

FOR: DATA COMMUNICATION OVER LOCAL NETWORKS, WIRELESS NETWORKS AND GLOBAL COMMUNICATIONS NETWORKS, INCLUDING THE INTERNET, INTRANETS, EXTRANETS, TELEVISION, MOBILE COMMUNICATION, CELLULAR AND SATELLITE NETWORKS, IN CLASS 38 (U.S. CLS. 100, 101 AND 104).

FIRST USE 2-19-2014; IN COMMERCE 2-19-2014.

FOR: ELECTRONIC STORAGE OF DATA, TEXT, IMAGES, AUDIO, VIDEO; STORAGE SERVICES FOR ARCHIVING ELECTRONIC DATA, IN CLASS 39 (U.S. CLS. 100 AND 105).

FIRST USE 2-19-2014; IN COMMERCE 2-19-2014.

FOR: APPLICATION SERVICE PROVIDER (ASP) SERVICES FEATURING SOFTWARE FOR AUTHORING, DOWNLOADING, TRANSMITTING, RECEIVING, EDITING, EXTRACTING, ENCODING, DECODING, DISPLAYING, STORING AND ORGANIZING TEXT, GRAPHICS, IMAGES, AND ELECTRONIC PUBLICATIONS, IN CLASS 42 (U.S. CLS. 100 AND 101).

FIRST USE 2-19-2014; IN COMMERCE 2-19-2014.

THE MARK CONSISTS OF STANDARD CHARACTERS WITHOUT CLAIM TO ANY PARTICULAR FONT, STYLE, SIZE, OR COLOR.

SER. NO. 85-916,372, FILED 4-26-2013.

Michelle K. Lee

Deputy Director of the United States Patent and Trademark Office

KATHY WANG, EXAMINING ATTORNEY

REQUIREMENTS TO MAINTAIN YOUR FEDERAL TRADEMARK REGISTRATION

WARNING: YOUR REGISTRATION WILL BE CANCELLED IF YOU DO NOT FILE THE DOCUMENTS BELOW DURING THE SPECIFIED TIME PERIODS.

Requirements in the First Ten Years*
What and When to File:

First Filing Deadline: You must file a Declaration of Use (or Excusable Nonuse) between the 5th and 6th years after the registration date. *See* 15 U.S.C. §§1058, 1141k. If the declaration is accepted, the registration will continue in force for the remainder of the ten-year period, calculated from the registration date, unless cancelled by an order of the Commissioner for Trademarks or a federal court.

Second Filing Deadline: You must file a Declaration of Use (or Excusable Nonuse) **and** an Application for Renewal between the 9th and 10th years after the registration date.* *See* 15 U.S.C. §1059.

Requirements in Successive Ten-Year Periods*
What and When to File:

You must file a Declaration of Use (or Excusable Nonuse) **and** an Application for Renewal between every 9th and 10th-year period, calculated from the registration date.*

Grace Period Filings*

The above documents will be accepted as timely if filed within six months after the deadlines listed above with the payment of an additional fee.

The United States Patent and Trademark Office (USPTO) will NOT send you any future notice or reminder of these filing requirements.

***ATTENTION MADRID PROTOCOL REGISTRANTS:** The holder of an international registration with an extension of protection to the United States under the Madrid Protocol must timely file the Declarations of Use (or Excusable Nonuse) referenced above directly with the USPTO. The time periods for filing are based on the U.S. registration date (not the international registration date). The deadlines and grace periods for the Declarations of Use (or Excusable Nonuse) are identical to those for nationally issued registrations. *See* 15 U.S.C. §§1058, 1141k. However, owners of international registrations do not file renewal applications at the USPTO. Instead, the holder must file a renewal of the underlying international registration at the International Bureau of the World Intellectual Property Organization, under Article 7 of the Madrid Protocol, before the expiration of each ten-year term of protection, calculated from the date of the international registration. *See* 15 U.S.C. §1141j. For more information and renewal forms for the international registration, see http://www.wipo.int/madrid/en/.

NOTE: Fees and requirements for maintaining registrations are subject to change. Please check the USPTO website for further information. With the exception of renewal applications for registered extensions of protection, you can file the registration maintenance documents referenced above online at http://www.uspto.gov.

United States of America

United States Patent and Trademark Office

Reg. No. 6,201,364

Registered Nov. 17, 2020

Int. Cl.: 9, 38, 42

Service Mark

Trademark

Principal Register

Microsoft Corporation (WASHINGTON CORPORATION)
One Microsoft Way
Redmond, WASHINGTON 98052

CLASS 9: Downloadable computer software for receiving, displaying, storing, organizing and sharing with other users documents, sounds, music, videos, photographs, drawings, images and data stored electronically

FIRST USE 4-9-2019; IN COMMERCE 4-9-2019

CLASS 38: Telecommunication services, namely, transmission of documents, sounds, music, videos, photographs, drawings, images and data by means of telecommunications networks, wireless communication networks, and the internet

FIRST USE 4-9-2019; IN COMMERCE 4-9-2019

CLASS 42: Providing temporary use of non-downloadable software for receiving, displaying, storing, organizing and sharing with other users documents, sounds, music, videos, photographs, drawings, images and data stored electronically; electronic storage of files and documents for others

FIRST USE 4-9-2019; IN COMMERCE 4-9-2019

The color(s) blue is/are claimed as a feature of the mark.

The mark consists of a stylized blue cloud.

SER. NO. 88-430,030, FILED 05-14-2019

Director of the United States
Patent and Trademark Office

REQUIREMENTS TO MAINTAIN YOUR FEDERAL TRADEMARK REGISTRATION

WARNING: YOUR REGISTRATION WILL BE CANCELLED IF YOU DO NOT FILE THE DOCUMENTS BELOW DURING THE SPECIFIED TIME PERIODS.

Requirements in the First Ten Years*
What and When to File:

- ***First Filing Deadline:*** You must file a Declaration of Use (or Excusable Nonuse) between the 5th and 6th years after the registration date. See 15 U.S.C. §§1058, 1141k. If the declaration is accepted, the registration will continue in force for the remainder of the ten-year period, calculated from the registration date, unless cancelled by an order of the Commissioner for Trademarks or a federal court.

- ***Second Filing Deadline:*** You must file a Declaration of Use (or Excusable Nonuse) and an Application for Renewal between the 9th and 10th years after the registration date.* See 15 U.S.C. §1059.

Requirements in Successive Ten-Year Periods*
What and When to File:

- You must file a Declaration of Use (or Excusable Nonuse) and an Application for Renewal between every 9th and 10th-year period, calculated from the registration date.*

Grace Period Filings*

The above documents will be accepted as timely if filed within six months after the deadlines listed above with the payment of an additional fee.

***ATTENTION MADRID PROTOCOL REGISTRANTS:** The holder of an international registration with an extension of protection to the United States under the Madrid Protocol must timely file the Declarations of Use (or Excusable Nonuse) referenced above directly with the United States Patent and Trademark Office (USPTO). The time periods for filing are based on the U.S. registration date (not the international registration date). The deadlines and grace periods for the Declarations of Use (or Excusable Nonuse) are identical to those for nationally issued registrations. See 15 U.S.C. §§1058, 1141k. However, owners of international registrations do not file renewal applications at the USPTO. Instead, the holder must file a renewal of the underlying international registration at the International Bureau of the World Intellectual Property Organization, under Article 7 of the Madrid Protocol, before the expiration of each ten-year term of protection, calculated from the date of the international registration. See 15 U.S.C. §1141j. For more information and renewal forms for the international registration, see http://www.wipo.int/madrid/en/.

NOTE: Fees and requirements for maintaining registrations are subject to change. Please check the USPTO website for further information. With the exception of renewal applications for registered extensions of protection, you can file the registration maintenance documents referenced above online at http://www.uspto.gov.

NOTE: A courtesy e-mail reminder of USPTO maintenance filing deadlines will be sent to trademark owners/holders who authorize e-mail communication and maintain a current e-mail address with the USPTO. To ensure that e-mail is authorized and your address is current, please use the Trademark Electronic Application System (TEAS) Correspondence Address and Change of Owner Address Forms available at http://www.uspto.gov.

United States of America

United States Patent and Trademark Office

Reg. No. 5,063,043

Registered Oct. 18, 2016

Int. Cl.: 9, 42

Service Mark

Trademark

Principal Register

Microsoft Corporation (WASHINGTON CORPORATION)
One Microsoft Way
Redmond, WA 980526399

CLASS 9: Word processing software; computer programs for creating, editing, sharing, storing, and printing documents comprised of text and graphics and utility programs for use therewith

FIRST USE 12-1-2012; IN COMMERCE 12-1-2012

CLASS 42: Cloud computing featuring word processing software; non-downloadable computer programs for creating, editing, sharing, storing, and printing documents comprised of text and graphics and utility programs for use therewith

FIRST USE 12-1-2012; IN COMMERCE 12-1-2012

The color(s) blue and white is/are claimed as a feature of the mark.

The mark consists of a stylized depiction of a blue rectangle with a white letter "W" in the center partially covering an adjacent image of a piece of white paper outlined in blue displaying horizontal lines across the paper featured in blue and white.

SER. NO. 86-928,345, FILED 03-03-2016
GEOFFREY A FOSDICK, EXAMINING ATTORNEY

Michelle K. Lee

Director of the United States
Patent and Trademark Office

REQUIREMENTS TO MAINTAIN YOUR FEDERAL TRADEMARK REGISTRATION

WARNING: YOUR REGISTRATION WILL BE CANCELLED IF YOU DO NOT FILE THE DOCUMENTS BELOW DURING THE SPECIFIED TIME PERIODS.

Requirements in the First Ten Years*
What and When to File:

- ***First Filing Deadline:*** You must file a Declaration of Use (or Excusable Nonuse) between the 5th and 6th years after the registration date. See 15 U.S.C. §§1058, 1141k. If the declaration is accepted, the registration will continue in force for the remainder of the ten-year period, calculated from the registration date, unless cancelled by an order of the Commissioner for Trademarks or a federal court.

- ***Second Filing Deadline:*** You must file a Declaration of Use (or Excusable Nonuse) and an Application for Renewal between the 9th and 10th years after the registration date.* See 15 U.S.C. §1059.

Requirements in Successive Ten-Year Periods*
What and When to File:

- You must file a Declaration of Use (or Excusable Nonuse) and an Application for Renewal between every 9th and 10th-year period, calculated from the registration date.*

Grace Period Filings*

The above documents will be accepted as timely if filed within six months after the deadlines listed above with the payment of an additional fee.

***ATTENTION MADRID PROTOCOL REGISTRANTS:** The holder of an international registration with an extension of protection to the United States under the Madrid Protocol must timely file the Declarations of Use (or Excusable Nonuse) referenced above directly with the United States Patent and Trademark Office (USPTO). The time periods for filing are based on the U.S. registration date (not the international registration date). The deadlines and grace periods for the Declarations of Use (or Excusable Nonuse) are identical to those for nationally issued registrations. See 15 U.S.C. §§1058, 1141k. However, owners of international registrations do not file renewal applications at the USPTO. Instead, the holder must file a renewal of the underlying international registration at the International Bureau of the World Intellectual Property Organization, under Article 7 of the Madrid Protocol, before the expiration of each ten-year term of protection, calculated from the date of the international registration. See 15 U.S.C. §1141j. For more information and renewal forms for the international registration, see http://www.wipo.int/madrid/en/.

NOTE: Fees and requirements for maintaining registrations are subject to change. Please check the USPTO website for further information. With the exception of renewal applications for registered extensions of protection, you can file the registration maintenance documents referenced above online at http://www.uspto.gov.

NOTE: A courtesy e-mail reminder of USPTO maintenance filing deadlines will be sent to trademark owners/holders who authorize e-mail communication and maintain a current e-mail address with the USPTO. To ensure that e-mail is authorized and your address is current, please use the Trademark Electronic Application System (TEAS) Correspondence Address and Change of Owner Address Forms available at http://www.uspto.gov.

United States of America
United States Patent and Trademark Office

MICROSOFT 365

Reg. No. 6,701,693

Registered Apr. 12, 2022

Int. Cl.: 9, 35, 37, 38, 41, 42

Service Mark

Trademark

Principal Register

Microsoft Corporation (WASHINGTON CORPORATION)
ONE MICROSOFT WAY
REDMOND, WASHINGTON 98052

CLASS 9: computer software and computer programs for database management, data storage and backup, virtualization, networking, collaboration, remote access, remote support, cloud computing, data sharing, data security, access, administration and management of computer applications and computer hardware, computer application distribution, and for transmission of voice, data, images, audio, video, and information, and for content management, online project management, creating, offering, hosting, and delivering online conferences, meetings, demonstrations, tours, presentations and interactive discussions, word processing programs, and operating system programs; computer software, namely, a full line of computer software for business productivity, business IT service management, business computer devices management, business IT security management, business administration and management, accounting, and marketing in the fields of business, and computer software to facilitate e-commerce business transactions via a global computer network; computer operating system software; network access server operating software; computer programs for managing communications and data exchange between computers and electronic devices; computer network security, anti-virus protection, and intrusion detection and prevention; computer graphics and graphical user interface software; wireless communications devices, namely, mobile phones, cellular telephones, personal digital assistants, and hand-held computers; computer software development tools; website development software; computer software that provides web-based access to applications and services through a web operating system or portal interface; computer software for developing and operating cloud computer networks and applications; computer software for computer system and application development, deployment and management; computer hardware and software for monitoring automobiles performance, for mapping and navigation, for electronic mail and wireless communications, for maintaining personal directories, contact lists, address and telephone number lists

FIRST USE 7-10-2017; IN COMMERCE 7-10-2017

CLASS 35: business services, namely, business consultation services, business advice and information services; business marketing services; and business consulting services; providing business information

Performing the Functions and Duties of the
Under Secretary of Commerce for Intellectual Property and
Director of the United States Patent and Trademark Office

FIRST USE 7-10-2017; IN COMMERCE 7-10-2017

CLASS 37: consultancy concerning installation, maintenance and repair of computer hardware

FIRST USE 7-10-2017; IN COMMERCE 7-10-2017

CLASS 38: telecommunications services, namely, providing on-line chat rooms for the transmission of messages among users in the field of general interest; voice chat services; electronic transmission and streaming of digital media, messages, documents, images, music, games and data; voice over internet protocol services; video-on-demand transmission services; providing online chat rooms and electronic bulletin boards for transmission of messages among users concerning business services, listings for announcements, events, meetings, activities, politics, family, arts and information on a wide variety of topics of general interest to the public and consultancy services, for all of the aforesaid services

FIRST USE 7-10-2017; IN COMMERCE 7-10-2017

CLASS 41: providing education and training services, namely, classes, seminars, workshops, and non-downloadable webinars in the field of computers and computer technology; arranging and conducting educational conferences and exhibitions in the field of computer technology; providing information over computer networks and global communication networks in the fields of entertainment, music, interactive games, movies, sports, news relating to current events, and arts and culture; information, advice and consultancy services relating to the aforesaid services

FIRST USE 7-10-2017; IN COMMERCE 7-10-2017

CLASS 42: computer services, namely, providing technical support, information and consultation services, namely, troubleshooting in the nature of diagnosing problems in computer hardware, computer software and computer operating systems; computer hardware and software testing services; computer services, namely, providing software updates via computer networks and global communication networks; computer services, namely, providing on-line non-downloadable software for database management, data storage and backup, virtualization, networking, collaboration, remote access, remote support, cloud computing, data sharing, data security, access, administration and management of computer applications and computer hardware, computer application distribution, and for transmission of voice, data, images, audio, video, and information, and for content management, online project management, creating, offering, hosting, and delivering online conferences, meetings, demonstrations, tours, presentations and interactive discussions, word processing programs, operating system programs; electronic data storage; cloud services, namely, providing on-line non-downloadable operating software for accessing and using a cloud computing network; cloud hosting provider services; computer security services, namely, enforcing, restricting and controlling access privileges of users of computing resources for cloud resources based on assigned credentials, integration of private and public cloud computing environments, remote and on-site infrastructure management services for monitoring, administration and management of public and private cloud computing it and application systems; providing virtual computer systems and virtual computer environments through cloud computing; application service provider (asp), namely, providing, hosting, managing, developing, and maintaining applications, software, web sites, and databases of others; providing technical information in the fields of design, development, programming, customization, selection, and implementation of computers, computer software, and computer networks, and information regarding diagnosing computer hardware and software problems and regarding the maintenance and updating of computer software, and the development and operation of computer systems, software and networks; computer software consulting services; consultancy in the design and development of computer hardware; consulting in the field of information technology; consulting in the field of cloud computing networks and

applications; design and development of networks and network software and applications; leasing computer facilities; electronic storage of files and documents; electronic storage of files, documents and databases; technology consultancy services in the field of development of computer software; platform-as-a-service (paas), infrastructure-as-a-service (iaas) and software-as-a-service (saas) services featuring computer software platforms for creating web applications, data storage and backup, database management, virtualization, networking, collaboration, remote access, remote support, cloud computing, data sharing, data security, access, administration and management of computer applications and computer hardware, computer application distribution, and for transmission of voice, data, images, audio, video, and information, and for content management, online project management, creating, offering, hosting, and delivering online conferences, meetings, demonstrations, tours, presentations and interactive discussions; computer services, namely, creating cloud-based indexes of information; computer hardware and software development

FIRST USE 7-10-2017; IN COMMERCE 7-10-2017

THE MARK CONSISTS OF STANDARD CHARACTERS WITHOUT CLAIM TO ANY PARTICULAR FONT STYLE, SIZE OR COLOR

PRIORITY CLAIMED UNDER SEC. 44(D) ON AZERBAIJAN APPLICATION NO. 201733579, FILED 05-17-2017

SER. NO. 87-640,393, FILED 10-10-2017

REQUIREMENTS TO MAINTAIN YOUR FEDERAL TRADEMARK REGISTRATION

WARNING: YOUR REGISTRATION WILL BE CANCELLED IF YOU DO NOT FILE THE DOCUMENTS BELOW DURING THE SPECIFIED TIME PERIODS.

Requirements in the First Ten Years*
What and When to File:

- ***First Filing Deadline:*** You must file a Declaration of Use (or Excusable Nonuse) between the 5th and 6th years after the registration date. See 15 U.S.C. §§1058, 1141k. If the declaration is accepted, the registration will continue in force for the remainder of the ten-year period, calculated from the registration date, unless cancelled by an order of the Commissioner for Trademarks or a federal court.

- ***Second Filing Deadline:*** You must file a Declaration of Use (or Excusable Nonuse) and an Application for Renewal between the 9th and 10th years after the registration date.* See 15 U.S.C. §1059.

Requirements in Successive Ten-Year Periods*
What and When to File:

- You must file a Declaration of Use (or Excusable Nonuse) and an Application for Renewal between every 9th and 10th-year period, calculated from the registration date.*

Grace Period Filings*

The above documents will be accepted as timely if filed within six months after the deadlines listed above with the payment of an additional fee.

***ATTENTION MADRID PROTOCOL REGISTRANTS:** The holder of an international registration with an extension of protection to the United States under the Madrid Protocol must timely file the Declarations of Use (or Excusable Nonuse) referenced above directly with the United States Patent and Trademark Office (USPTO). The time periods for filing are based on the U.S. registration date (not the international registration date). The deadlines and grace periods for the Declarations of Use (or Excusable Nonuse) are identical to those for nationally issued registrations. See 15 U.S.C. §§1058, 1141k. However, owners of international registrations do not file renewal applications at the USPTO. Instead, the holder must file a renewal of the underlying international registration at the International Bureau of the World Intellectual Property Organization, under Article 7 of the Madrid Protocol, before the expiration of each ten-year term of protection, calculated from the date of the international registration. See 15 U.S.C. §1141j. For more information and renewal forms for the international registration, see http://www.wipo.int/madrid/en/.

NOTE: Fees and requirements for maintaining registrations are subject to change. Please check the USPTO website for further information. With the exception of renewal applications for registered extensions of protection, you can file the registration maintenance documents referenced above online at http://www.uspto.gov.

NOTE: A courtesy e-mail reminder of USPTO maintenance filing deadlines will be sent to trademark owners/holders who authorize e-mail communication and maintain a current e-mail address with the USPTO. To ensure that e-mail is authorized and your address is current, please use the Trademark Electronic Application System (TEAS) Correspondence Address and Change of Owner Address Forms available at http://www.uspto.gov.

United States of America
United States Patent and Trademark Office

OFFICE 365

Reg. No. 4,380,754

Registered Aug. 6, 2013

Int. Cl.: 39

SERVICE MARK

PRINCIPAL REGISTER

MICROSOFT CORPORATION (WASHINGTON CORPORATION)
ONE MICROSOFT WAY
REDMOND, WA 980526399

FOR: ELECTRONIC STORAGE OF FILES AND DOCUMENTS, IN CLASS 39 (U.S. CLS. 100 AND 105).

FIRST USE 10-19-2010; IN COMMERCE 10-19-2010.

THE MARK CONSISTS OF STANDARD CHARACTERS WITHOUT CLAIM TO ANY PARTICULAR FONT, STYLE, SIZE, OR COLOR.

OWNER OF U.S. REG. NOS. 2,841,438, 3,625,391, AND OTHERS.

NO CLAIM IS MADE TO THE EXCLUSIVE RIGHT TO USE "OFFICE", APART FROM THE MARK AS SHOWN.

SN 85-467,634, FILED 11-8-2011.

SETH A. RAPPAPORT, EXAMINING ATTORNEY

Acting Director of the United States Patent and Trademark Office

REQUIREMENTS TO MAINTAIN YOUR FEDERAL TRADEMARK REGISTRATION

WARNING: YOUR REGISTRATION WILL BE CANCELLED IF YOU DO NOT FILE THE DOCUMENTS BELOW DURING THE SPECIFIED TIME PERIODS.

Requirements in the First Ten Years*
What and When to File:

First Filing Deadline: You must file a Declaration of Use (or Excusable Nonuse) between the 5th and 6th years after the registration date. *See* 15 U.S.C. §§1058, 1141k. If the declaration is accepted, the registration will continue in force for the remainder of the ten-year period, calculated from the registration date, unless cancelled by an order of the Commissioner for Trademarks or a federal court.

Second Filing Deadline: You must file a Declaration of Use (or Excusable Nonuse) **and** an Application for Renewal between the 9th and 10th years after the registration date.* *See* 15 U.S.C. §1059.

Requirements in Successive Ten-Year Periods*
What and When to File:

You must file a Declaration of Use (or Excusable Nonuse) **and** an Application for Renewal between every 9th and 10th-year period, calculated from the registration date.*

Grace Period Filings*

The above documents will be accepted as timely if filed within six months after the deadlines listed above with the payment of an additional fee.

The United States Patent and Trademark Office (USPTO) will NOT send you any future notice or reminder of these filing requirements.

***ATTENTION MADRID PROTOCOL REGISTRANTS:** The holder of an international registration with an extension of protection to the United States under the Madrid Protocol must timely file the Declarations of Use (or Excusable Nonuse) referenced above directly with the USPTO. The time periods for filing are based on the U.S. registration date (not the international registration date). The deadlines and grace periods for the Declarations of Use (or Excusable Nonuse) are identical to those for nationally issued registrations. *See* 15 U.S.C. §§1058, 1141k. However, owners of international registrations do not file renewal applications at the USPTO. Instead, the holder must file a renewal of the underlying international registration at the International Bureau of the World Intellectual Property Organization, under Article 7 of the Madrid Protocol, before the expiration of each ten-year term of protection, calculated from the date of the international registration. *See* 15 U.S.C. §1141j. For more information and renewal forms for the international registration, see http://www.wipo.int/madrid/en/.

NOTE: Fees and requirements for maintaining registrations are subject to change. Please check the USPTO website for further information. With the exception of renewal applications for registered extensions of protection, you can file the registration maintenance documents referenced above online at http://www.uspto.gov.

Int. Cls.: 35 and 38

Prior U.S. Cls.: 100, 101, 102 and 104

United States Patent and Trademark Office

Reg. No. 2,165,601

Registered June 16, 1998

SERVICE MARK
PRINCIPAL REGISTER

HOTMAIL

HOTMAIL CORPORATION (CALIFORNIA CORPORATION)
1290 OAKMEAD PARKWAY, SUITE 218
SUNNYVALE, CA 94086

FOR: ADVERTISING AND MARKETING SERVICES, NAMELY, PROMOTING THE GOODS AND SERVICES OF OTHERS BY PLACING ADVERTISEMENTS AND PROMOTIONAL DISPLAYS IN AN ELECTRONIC SITE ACCESSED THROUGH COMPUTER NETWORKS AND BY DELIVERING ADVERTISEMENTS AND PROMOTIONAL MATERIALS TO OTHERS VIA ELECTRONIC MAIL, IN CLASS 35 (U.S. CLS. 100, 101 AND 102).

FIRST USE 7-4-1996; IN COMMERCE 7-4-1996.

FOR: ELECTRONIC MAIL SERVICES, IN CLASS 38 (U.S. CLS. 100, 101 AND 104).

FIRST USE 7-4-1996; IN COMMERCE 7-4-1996.

SER. NO. 75-272,783, FILED 4-10-1997.

EDWARD NELSON, EXAMINING ATTORNEY

APPENDIX C

United States of America

United States Patent and Trademark Office

Reg. No. 6,734,111

Registered May 24, 2022

Int. Cl.: 36, 41, 45

Service Mark

Principal Register

Carnegie Corporation of New York (NEW YORK non-profit corporation)
437 Madison Avenue
New York, NEW YORK 10022

CLASS 36: Charitable grantmaking, namely, providing grants for the support and promotion of education, democracy, international peace and security in the United States and Africa and higher education and research in Africa

FIRST USE 00-00-2014; IN COMMERCE 00-00-2014

CLASS 41: Providing a website featuring information in the field of education and higher education in the United States and Africa and research regarding education in Africa; providing online newsletters in the fields of education, democracy, international peace and security, and higher education in the United States and Africa, and educational research in Africa

FIRST USE 00-00-2014; IN COMMERCE 00-00-2014

CLASS 45: Providing a website featuring information in the fields of democracy, international peace and security in the United States and Africa

FIRST USE 00-00-2014; IN COMMERCE 00-00-2014

The mark consists of the script word "Carnegie" that is underlined. Below is the word "CORPORATION" which is above the wording "OF NEW YORK".

No claim is made to the exclusive right to use the following apart from the mark as shown: "CORPORATION OF NEW YORK"

SER. NO. 88-754,785, FILED 01-10-2020

Katherine Kelly Vidal

Director of the United States
Patent and Trademark Office

REQUIREMENTS TO MAINTAIN YOUR FEDERAL TRADEMARK REGISTRATION

WARNING: YOUR REGISTRATION WILL BE CANCELLED IF YOU DO NOT FILE THE DOCUMENTS BELOW DURING THE SPECIFIED TIME PERIODS.

Requirements in the First Ten Years*
What and When to File:

- ***First Filing Deadline:*** You must file a Declaration of Use (or Excusable Nonuse) between the 5th and 6th years after the registration date. See 15 U.S.C. §§1058, 1141k. If the declaration is accepted, the registration will continue in force for the remainder of the ten-year period, calculated from the registration date, unless cancelled by an order of the Commissioner for Trademarks or a federal court.

- ***Second Filing Deadline:*** You must file a Declaration of Use (or Excusable Nonuse) and an Application for Renewal between the 9th and 10th years after the registration date.* See 15 U.S.C. §1059.

Requirements in Successive Ten-Year Periods*
What and When to File:

- You must file a Declaration of Use (or Excusable Nonuse) and an Application for Renewal between every 9th and 10th-year period, calculated from the registration date.*

Grace Period Filings*

The above documents will be accepted as timely if filed within six months after the deadlines listed above with the payment of an additional fee.

***ATTENTION MADRID PROTOCOL REGISTRANTS:** The holder of an international registration with an extension of protection to the United States under the Madrid Protocol must timely file the Declarations of Use (or Excusable Nonuse) referenced above directly with the United States Patent and Trademark Office (USPTO). The time periods for filing are based on the U.S. registration date (not the international registration date). The deadlines and grace periods for the Declarations of Use (or Excusable Nonuse) are identical to those for nationally issued registrations. See 15 U.S.C. §§1058, 1141k. However, owners of international registrations do not file renewal applications at the USPTO. Instead, the holder must file a renewal of the underlying international registration at the International Bureau of the World Intellectual Property Organization, under Article 7 of the Madrid Protocol, before the expiration of each ten-year term of protection, calculated from the date of the international registration. See 15 U.S.C. §1141j. For more information and renewal forms for the international registration, see http://www.wipo.int/madrid/en/.

NOTE: Fees and requirements for maintaining registrations are subject to change. Please check the USPTO website for further information. With the exception of renewal applications for registered extensions of protection, you can file the registration maintenance documents referenced above online at http://www.uspto.gov.

NOTE: A courtesy e-mail reminder of USPTO maintenance filing deadlines will be sent to trademark owners/holders who authorize e-mail communication and maintain a current e-mail address with the USPTO. To ensure that e-mail is authorized and your address is current, please use the Trademark Electronic Application System (TEAS) Correspondence Address and Change of Owner Address Forms available at http://www.uspto.gov.

United States of America
United States Patent and Trademark Office

CARNEGIE CORPORATION OF NEW YORK

Reg. No. 6,734,112

Registered May 24, 2022

Int. Cl.: 36, 41, 45

Service Mark

Principal Register

Carnegie Corporation of New York (NEW YORK non-stock corporation)
437 Madison Avenue
New York, NEW YORK 10022

CLASS 36: Charitable grantmaking, namely, providing grants for the support and promotion of education, democracy, international peace and security in the United States and Africa and higher education and research in Africa

FIRST USE 00-00-1911; IN COMMERCE 00-00-1911

CLASS 41: Providing a website featuring information in the field of education and higher education in the United States and Africa and research regarding education in Africa; providing online newsletters in the fields of education, democracy, international peace and security, and higher education in the United States and Africa, and educational research in Africa

FIRST USE 00-00-1911; IN COMMERCE 00-00-1911

CLASS 45: Providing a website featuring information in the fields of democracy, international peace and security in the United States and Africa

FIRST USE 00-00-1911; IN COMMERCE 00-00-1911

THE MARK CONSISTS OF STANDARD CHARACTERS WITHOUT CLAIM TO ANY PARTICULAR FONT STYLE, SIZE OR COLOR

No claim is made to the exclusive right to use the following apart from the mark as shown: "CORPORATION OF NEW YORK"

SER. NO. 88-754,815, FILED 01-10-2020

Katherine Kelly Vidal

Director of the United States
Patent and Trademark Office

REQUIREMENTS TO MAINTAIN YOUR FEDERAL TRADEMARK REGISTRATION

WARNING: YOUR REGISTRATION WILL BE CANCELLED IF YOU DO NOT FILE THE DOCUMENTS BELOW DURING THE SPECIFIED TIME PERIODS.

Requirements in the First Ten Years*
What and When to File:

- ***First Filing Deadline:*** You must file a Declaration of Use (or Excusable Nonuse) between the 5th and 6th years after the registration date. See 15 U.S.C. §§1058, 1141k. If the declaration is accepted, the registration will continue in force for the remainder of the ten-year period, calculated from the registration date, unless cancelled by an order of the Commissioner for Trademarks or a federal court.

- ***Second Filing Deadline:*** You must file a Declaration of Use (or Excusable Nonuse) and an Application for Renewal between the 9th and 10th years after the registration date.* See 15 U.S.C. §1059.

Requirements in Successive Ten-Year Periods*
What and When to File:

- You must file a Declaration of Use (or Excusable Nonuse) and an Application for Renewal between every 9th and 10th-year period, calculated from the registration date.*

Grace Period Filings*

The above documents will be accepted as timely if filed within six months after the deadlines listed above with the payment of an additional fee.

***ATTENTION MADRID PROTOCOL REGISTRANTS:** The holder of an international registration with an extension of protection to the United States under the Madrid Protocol must timely file the Declarations of Use (or Excusable Nonuse) referenced above directly with the United States Patent and Trademark Office (USPTO). The time periods for filing are based on the U.S. registration date (not the international registration date). The deadlines and grace periods for the Declarations of Use (or Excusable Nonuse) are identical to those for nationally issued registrations. See 15 U.S.C. §§1058, 1141k. However, owners of international registrations do not file renewal applications at the USPTO. Instead, the holder must file a renewal of the underlying international registration at the International Bureau of the World Intellectual Property Organization, under Article 7 of the Madrid Protocol, before the expiration of each ten-year term of protection, calculated from the date of the international registration. See 15 U.S.C. §1141j. For more information and renewal forms for the international registration, see http://www.wipo.int/madrid/en/.

NOTE: Fees and requirements for maintaining registrations are subject to change. Please check the USPTO website for further information. With the exception of renewal applications for registered extensions of protection, you can file the registration maintenance documents referenced above online at http://www.uspto.gov.

NOTE: A courtesy e-mail reminder of USPTO maintenance filing deadlines will be sent to trademark owners/holders who authorize e-mail communication and maintain a current e-mail address with the USPTO. To ensure that e-mail is authorized and your address is current, please use the Trademark Electronic Application System (TEAS) Correspondence Address and Change of Owner Address Forms available at http://www.uspto.gov.