**IN THE UNITED STATES DISTRICT COURT**
**FOR THE EASTERN DISTRICT OF VIRGINIA**
**Alexandria Division**

| | |
|---|---|
| MICROSOFT CORPORATION, a Washington corporation,<br><br>Plaintiff,<br><br>v.<br><br>JOHN DOES 1-2, CONTROLLING A COMPUTER NETWORK AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS,<br><br>Defendants. | Civil Action No: 1:21-cv-822 |

**DECLARATION OF DONAL KEATING IN SUPPORT OF MICROSOFT'S APPLICATION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

I, Donal Keating, declare as follows:

1. I am the Director of Innovation and Research for Microsoft Corporation's Digital Crimes Unit ("DCU") within the company's Corporate, External, and Legal Affairs ("CELA") department. I make this declaration in support of Microsoft'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 and based on my review of records Microsoft maintains in the ordinary course of business. If called as a witness, I could and would testify competently to the truth of the matters set forth herein.

## I. INTRODUCTION

2. In my role at Microsoft, I personally oversee, coordinate and participate in investigations and mitigation efforts regarding activity that jeopardizes the integrity of Microsoft's systems and the safety of customer data. Through this work, I became personally

familiar with a very serious body of cybercrime infrastructure that is being used by a group of cybercriminals to target Microsoft's Office 365 ("O365") customers and services (and in turn their networks, vendors, contractors, and agents). In particular, Microsoft has discovered a sophisticated online criminal network that is attacking Microsoft, O365, and its customers through malicious "homoglyph" domains that unlawfully impersonate legitimate Microsoft O365 customers and their businesses. Homoglyph attacks rely on elaborate deception that leverages the similarities of character scripts to create imposter domains used to deceive unsuspecting individuals. Defendants use malicious homoglyph domains together with stolen customer credentials to unlawfully access customer accounts, monitor customer email traffic, gather intelligence on pending financial transactions, and criminally impersonate O365 customers, all in an attempt to deceive their victims into transferring funds to the cybercriminals. I am also personally familiar with the significant efforts that Microsoft takes to protect against such harms. Before joining Microsoft, I spent over a decade working in the software supply chain where I gained depth of experience which enabled me to work with Microsoft on combating software piracy and the illegal reproduction of Microsoft products including counterfeit identification and anti-piracy technology. I have been employed by Microsoft since 1998 where I have focused on protecting against illegal copying and distribution of intellectual property, conducting forensic investigations of cybercrime and protecting Microsoft customers from cybercrime.

## II. OVERVIEW OF INVESTIGATION INTO DEFENDANTS

### Overview Of Defendants' Scheme

3. My declaration concerns sophisticated criminals engaged in a complex scheme to target Microsoft's O365 customers and services and conduct malicious activity including business email compromise attacks ("BEC"), using stolen credentials to access O365 customer email accounts, imitate customer employees, and target their trusted networks, vendors,

contractors, and agents in an effort to deceive them into sending or approving fraudulent financial payments.

4. Defendants' attack typically unfolds as follows:

5. In the first phase, Doe Defendants use stolen O365 login credentials, typically obtained through deceptive efforts like credential phishing emails which enables unauthorized access to Microsoft's customers' O365 accounts.

6. In the second phase, after using stolen customer credentials to gain unauthorized access to the compromised Office 365 account, Defendants begin reconnaissance, which includes monitoring the compromised account, emails, and contact list to identify opportunities to target the compromised O365 customer's contacts for financial fraud, which may also include forwarding emails with key financial words like "invoice," "accounts receivable," "funds," "overdue," "payroll," or "IBAN," and masking their activities to evade detection.

7. In the final phase, having used stolen credentials to gain unauthorized access to Office 365 accounts and having monitored account activity, Defendants identify additional victims either in the compromised O365 customer's business or their wider network (typically, customers, vendors, or agents), who routinely deal with wire transfer requests, invoices, or billing statements and could be deceived by fraudulent requests for payment imitating legitimate payment communications. In this final phase, Defendants register homoglyph domains to impersonate legitimate businesses (hereinafter, "homoglyph imposter domains"), host these homoglyph imposter domains on a fraudulently procured O365 tenant, establish spoof email addresses impersonating one or more of the foregoing parties, all of which is designed to enable Defendants to deceive such parties into sending wire payments to Defendants. In all cases, the Defendants use fraudulent information to direct funds to themselves.

**Overview Of Defendants**

8. The precise identities and locations of the cybercriminals behind this unlawful scheme are generally unknown, but they targeted Microsoft customers and their networks across the globe including those located in Virginia and did so by registering homoglyph imposter domains through domain registries located in the Eastern District of Virginia. These cybercriminals are named as John Does 1 and 2 in this case (referred to here as "Defendants").

9. I investigated the technical infrastructure described in this declaration. During my investigation, I reviewed a publicly available database of information, called a "WHOIS" database. The WHOIS database generally contains the names, mailing addresses, email addresses and similar contact information provided by parties when registering domain names. I determined that the Defendants registered Internet domains using means that obfuscate their identities. In some cases, Defendants registered domains through private registration services, which conceal the contact information ordinarily available in the WHOIS database. In other cases, Defendants registered domains using free e-mail addresses that do not provide any indication of the registrants' identities. To the extent that other contact information is visible, I have not been able to associate such information to any real individual. On some occasions, for the private registration services, where WHOIS information is ordinarily concealed, Defendants are sometimes assigned arbitrary "proxy" email addresses associated with domain names and make those email addresses available in the public WHOIS database. The private registration services provide the proxy email addresses publicly for the purpose of enabling communication with Defendants regarding their domain names. Thus, for each domain, there is an email address that serves as a known point of contact with the Defendants. In both cases, I believe that the email addresses are the only known possible way of communicating the existence of

this action specifically to the Defendants.

**Overview Of Microsoft's Protective Efforts to Protect Customers And Defendants' Attempts to Evade Such Efforts**

10. Microsoft commits tremendous resources to protect its online services and works with customers to detect and prevent threats their accounts and data. Microsoft recently detected evidence of Defendants' malicious activity and promptly began to identify patterns and attempted to block Defendants' activity through the technical tools at its disposal. Defendants' activities victimize Microsoft's customers in two ways – first, they use stolen credentials to gain unauthorized access to and compromise accounts of O365 customers ("compromised account victim"), and second, they use this unauthorized access to O365 accounts to exfiltrate information and develop intelligence about financial transactions from the compromised account victim's wider network – including customers, vendors, or agents ("financial fraud victims") whether they are other O365 users or users of other email platforms. Defendants frequently target senior managers, financial roles (accountants, bookkeepers, etc.), and sales positions (purchasing and services) in a variety of industries.

11. Further, according to my investigation, to the extent Defendants have registered homoglyph imposter domains and are hosting those homoglyph imposter on O365 tenants that Defendants have fraudulently set up to carry out their criminal schemes, Microsoft takes steps to identify and block the ability of Defendants to use such fraudulent tenants and related accounts for malicious purposes.

12. Yet, even with such self-help measures, the risk of irreparable harm still exists because, even after Microsoft prevents and disables use of O365 for this fraud, Defendants are nonetheless able to move these fraudulent imposter domains to other third-party domain registrars and hosting facilities outside the Microsoft ecosystem. In this way, Defendants are

then able to continue criminal activities directed at Microsoft and O365 customers. It is also possible that Defendants register domains and host them from inception outside of Microsoft's ecosystem, placing them beyond Microsoft's internal mitigation measures. In all such scenarios, by maintaining access and control of these homoglyph imposter domains through third-party domain registrars and hosting companies, Defendants continue to target Microsoft's customers and others for financial fraud and other cybercrime.

13. There is a substantial risk from this situation that, notwithstanding Microsoft's significant steps to disable and block malicious infrastructure, Microsoft's customers may incorrectly blame Microsoft for Defendants' continued ability to use homoglyph imposter domains to target them for fraud and may incorrectly associate Microsoft with the harm caused by Defendants.

14. Defendants' ability to mobilize and move malicious domains presents an ongoing threat to Microsoft's customers and others and undermines Microsoft's efforts to protect its customers and networks. Without the relief requested from this Court, Microsoft will be engaged in a constant game of whack-a-mole where it attempts to protect its customers by shutting down Defendants' malicious activity using tools at its disposal within O365, only to have Defendants move their malicious domains to another domain registrar or hosting company, where the domain can be administered and email services set up by Defendants on other companies' email services, thus enabling Defendants to continue their attacks against Microsoft and Microsoft customers and their networks. This risk is not theoretical, as there is already evidence that Defendants have moved one of the domains from the O365 environment to another hosting company and thereby taken it outside Microsoft's reach.

15. Defendants continue to evolve their tactics in an attempt to avoid detection by

Microsoft's customers and to evade Microsoft's numerous safeguards. Given the risk posed by Defendants reconstituting and moving their operations to commit further malicious acts, Defendants pose a current and ongoing threat to Microsoft and the security of its customers such that it is necessary to seek immediate relief in this action.

## III. MICROSOFT'S OFFICE 365 SERVICES AND PROTECTION MEASURES

16. Office 365 is an online service that provides, among other things, access to Microsoft's Office software on a subscription basis. Customers purchase a subscription to Office 365 that may provide access to both cloud and locally stored versions of the software. Use of Office 365 requires an online account.

17. Microsoft goes to great lengths to protect customer accounts. In particular, Microsoft engineered Office 365 with the intent to eliminate threats before reaching Office 365 users. Microsoft uses real-time anti-spam and multiple anti-malware engines to prevent threats from reaching their inboxes. Microsoft also offers Microsoft Defender for Office 365,[1] which helps protect customers against new, sophisticated attacks in real time. In addition to incorporating tools to stop phishing emails before they reach users, Microsoft also investigates the underlying phishing attacks to identify and prevent malicious attacks carried out by criminal organizations.

## IV. DEFENDANTS USE UNAUTHORIZED ACCESS TO MICROSOFT OFFICE 365 CUSTOMERS' ACCOUNTS TO TARGET THEIR BUSINESSES AND LARGER NETWORKS

18. Through various investigative techniques, including those summarized above, Microsoft recently uncovered Defendants' scheme to gain unauthorized access and compromise

[1] *See generally* https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-advanced-threat-protection-service-description.

O365 accounts, create homoglyph imposter domains, and use this malicious infrastructure and surveillance efforts to target compromised account victim's wider network – including customers, vendors, or agents – for fraudulent financial transactions. I participated in the investigation of Defendants' conduct and am personally familiar with the details of Microsoft's investigation in this case.

**Phase One: Unauthorized Access to Office 365 Using Stolen Credentials**

19. The first phase of the business email compromise scheme involves stealing Microsoft O365 credentials through among other means sending credential phishing emails and using malicious websites to socially engineer victims into divulging their account login credentials.

20. In my experience, credentials are most typically stolen through an attacker sending a "phishing" email to the victim that contains a link to a malicious website used to socially engineer victims into divulging their account login credentials. Attackers accomplish this by using email domains chosen to impersonate trusted domains or appear otherwise legitimate, and malicious websites set up to impersonate legitimate Microsoft login pages (*e.g.,* using trademark/copyright infringing images to spoof a legitimate Microsoft landing page). The attackers' goal is to deceive targeted victims such that they visit the malicious site and enter their Office 365 account credentials into a counterfeit login page, and those credentials are then captured for subsequent use by the attacker. These types of malicious attacks persist despite the fact that Microsoft encourages all its customers to use certain precautions to protect account credentials such as enabling two factor authentication. Regardless of the method of compromise, Defendants' subsequent use of the stolen credentials to unlawfully access accounts can be identified and observed.

21. Defendants, who make unauthorized access to Office 365 accounts, may engage in the initial phishing activities to obtain credentials to access those accounts or they may acquire such stolen credentials from other cybercriminals. At this juncture, Microsoft does not know which approach Defendants have taken. Nonetheless, Defendants ultimately have in their possession stolen Office 365 credentials which are used for malicious purposes described herein. Regardless of whether Defendants engaged in the initial theft of the credentials or purchased stolen credentials, Defendants are using such credentials to cause severe harm to Microsoft and its customers.

**Phase Two: Monitoring Compromised Office 365 Account Email Traffic and Contacts to Identify Opportunities for Further Criminal Activities**

22. In the second phase, once Defendants unlawfully gain access to an Office 365 account using stolen credentials, they begin reconnaissance of the compromised account and the compromised account victim's networks in a few ways. Defendants go through the compromised account victim's Office 365 email mailboxes, stored contacts, and address books to identify opportunities to target customers, vendors, and agents within the compromised account owner's network to solicit fraudulent financial transactions.

23. Defendants either directly monitor the contents of the mailbox or engage in "forwarding" of emails in the compromised email account in order to identify and review communications regarding financial transactions. For example, Defendants access or forward emails containing keywords such as "invoice," "accounts receivable," "funds," "overdue," "payroll," or "IBAN." Defendants either directly access or forward emails with keywords to a collection email account controlled and monitored by Defendants for further analysis. In an effort to avoid detection, Defendants may use unauthorized access to the account to mark any alerts or warnings about their activity as "read" and hiding their changes to the account to avoid

detection and alerting the owner of the compromised O365 account.

24. Defendants identify key emails and senders to impersonate and identify recipients to target. Defendants then register malicious imposter domains and spoof email addresses on those domains. Defendants use these homoglyph imposter domains and email addresses to fraudulently insert themselves into ongoing business transactions or socially engineer opportunities to interact with the financial or billing department of victims. Defendants take advantage of the fact that these emails are designed to appear legitimate and imitate legitimate email addresses that are trusted or known contacts of the recipient, and are part of existing, legitimate communications.

25. Once they have used stolen credentials to access O365 accounts, Defendants are opportunistic in identifying potential financial fraud victims – anyone who might be mentioned in emails, contact lists, or other communications in the compromised account users' account – and widen the pool of their victims beyond O365 to other email platforms outside of Microsoft's control.

**Phase Three: Impersonating O365 Account Owners or Members of Their Networks to Solicit Fraudulent Financial Transactions**

26. In the final phase, having analyzed e-mail traffic from multiple endpoints and monitored for upcoming financial transactions, invoices, bank payment information, or payment details, Defendants set up homoglyph imposter domains together with spoofed email addresses to impersonate O365 account owners or members of their networks and solicit fraudulent financial transactions.

27. Defendants use unlawful access to the compromised O365 account and its content to build out the necessary malicious infrastructure to launch attacks including registering one or more homoglyph imposter domains and creating email addresses that impersonate real people

identified during the reconnaissance phase.

28. Defendants create malicious domains that are "homoglyphs" of legitimate domain names. Homoglyphs are a technique by which attackers abuse similarities of character scripts to create deceptively similar domains. For example, a homoglyph domain may utilize characters with shapes that appear identical or very similar to the characters of a legitimate domain. Defendants' efforts to imitate legitimate domains using fraudulent homoglyph variants are clear from the examples below:

- **Defendants add adding a single letter**:

| **Legitimate** | **Impersonation** |
|---|---|
| junctionfueling.com | junctionfuelings.com (Adds an "s") |

- **Defendants replace letters with similar appearing letters**:

| **Legitimate** | **Impersonation** |
|---|---|
| leaseaccelerator.com | leaseacceierator.com (Changes "l" to "i") |
| lithiumamericas.com | lithlumamericas.com (Changes "i" to "l") |
| sliao.ca | sllao.ca (Changes "i" to "l") |

- **Defendants change top level domain information**:

| **Legitimate** | **Impersonation** |
|---|---|
| ccp.edu | ccp-edu.com (Adds .com) |

29. Once Defendants' homoglyph imposter domains are registered and operational, they can send spoofed emails from these homoglyph imposter domains which impersonate the compromised account victim or other legitimate contacts of the target – who might typically respond to requests to pay wire transfer requests, invoices, or billing statements.

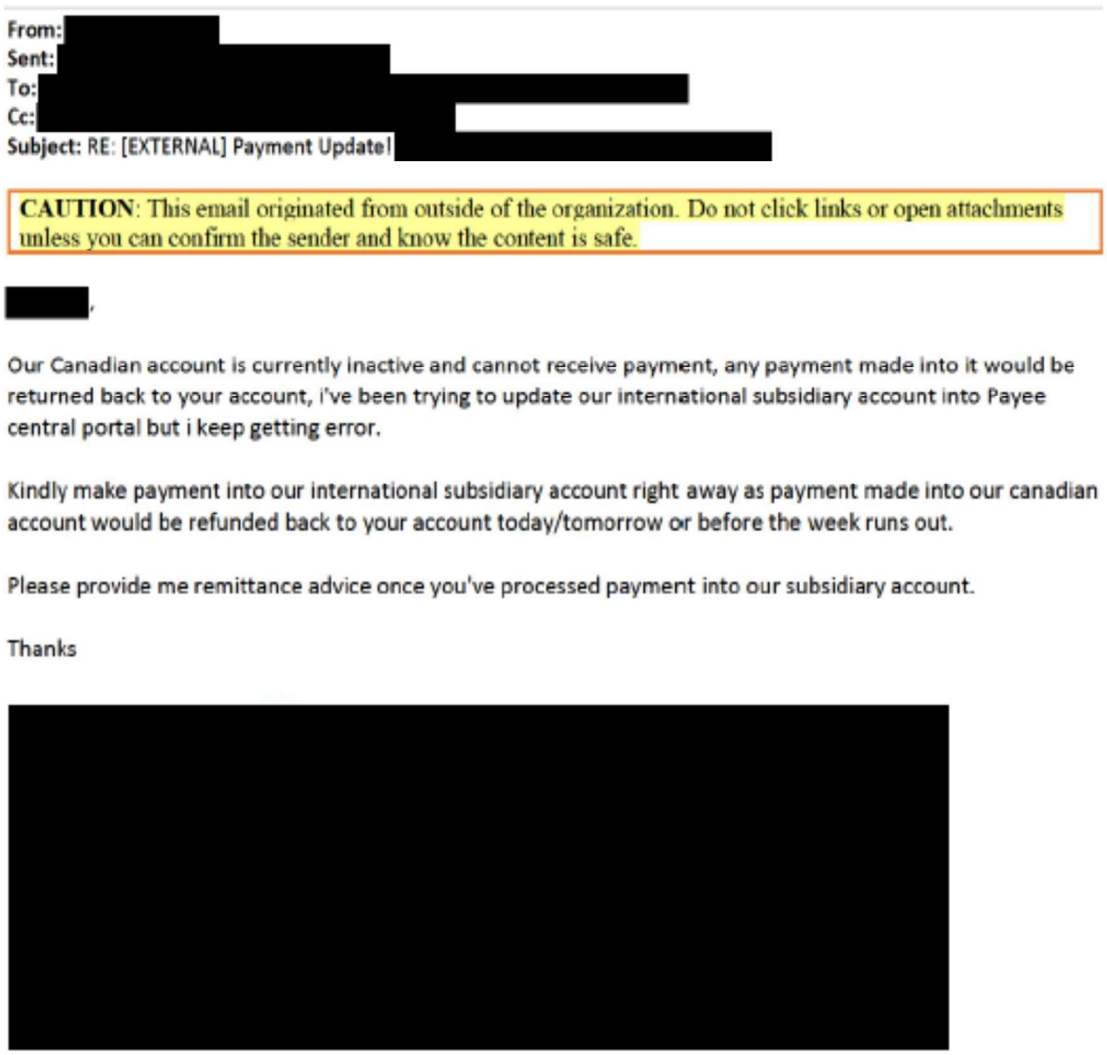
30. Defendants, leveraging unauthorized access to the O365 account, can copy the entire body of a prior legitimate email chain, use identical names and signature blocks, but send the impersonation email from a spoofed email address from a homoglyph mail exchange domain which impersonates a legitimate Microsoft O365 customer.

31. Defendants' fraudulent email communications build on existing, legitimate email communications, course of dealings, or business relationships. Defendants have access to prior email chains, can familiarize themselves with key terminology or terms of art, relevant documents, invoices, or account numbers. Defendants have unauthorized access to information that enables them to leverage existing conversations to try to convince victims to reveal critical business or financial information or process or redirect a payment request or invoice. Defendants commonly use an excuse about why new financial transfer information is being provided or threaten the victim for failure to provide payment or other strategies to create urgency and justify new payment arrangements. These strategies often include providing doctored invoice documents and tampered banking information. The financial fraud victims have no reason to suspect anything malicious, as the email appears to be from a known, legitimate email address, references existing conversations or prior communications, and provides doctored imitations of real financial documents.

32. In all cases, the Defendants use fraudulent information to unlawfully direct funds to themselves.

33. One example of a business compromise email sent in this case is included below and demonstrates how it mirrors genuine email traffic and instructs the financial fraud victim to redirect an invoice payment:

34. Defendants identified a legitimate email communication from the compromised account of an Office 365 customer referencing payment issues and asking for advice on processing payment:



From: [redacted]
Sent: [redacted]
To: [redacted]
Cc: [redacted]
Subject: RE: [EXTERNAL] Payment Update! [redacted]

**CAUTION**: This email originated from outside of the organization. Do not click links or open attachments unless you can confirm the sender and know the content is safe.

[redacted],

Our Canadian account is currently inactive and cannot receive payment, any payment made into it would be returned back to your account, i've been trying to update our international subsidiary account into Payee central portal but i keep getting error.

Kindly make payment into our international subsidiary account right away as payment made into our canadian account would be refunded back to your account today/tomorrow or before the week runs out.

Please provide me remittance advice once you've processed payment into our subsidiary account.

Thanks

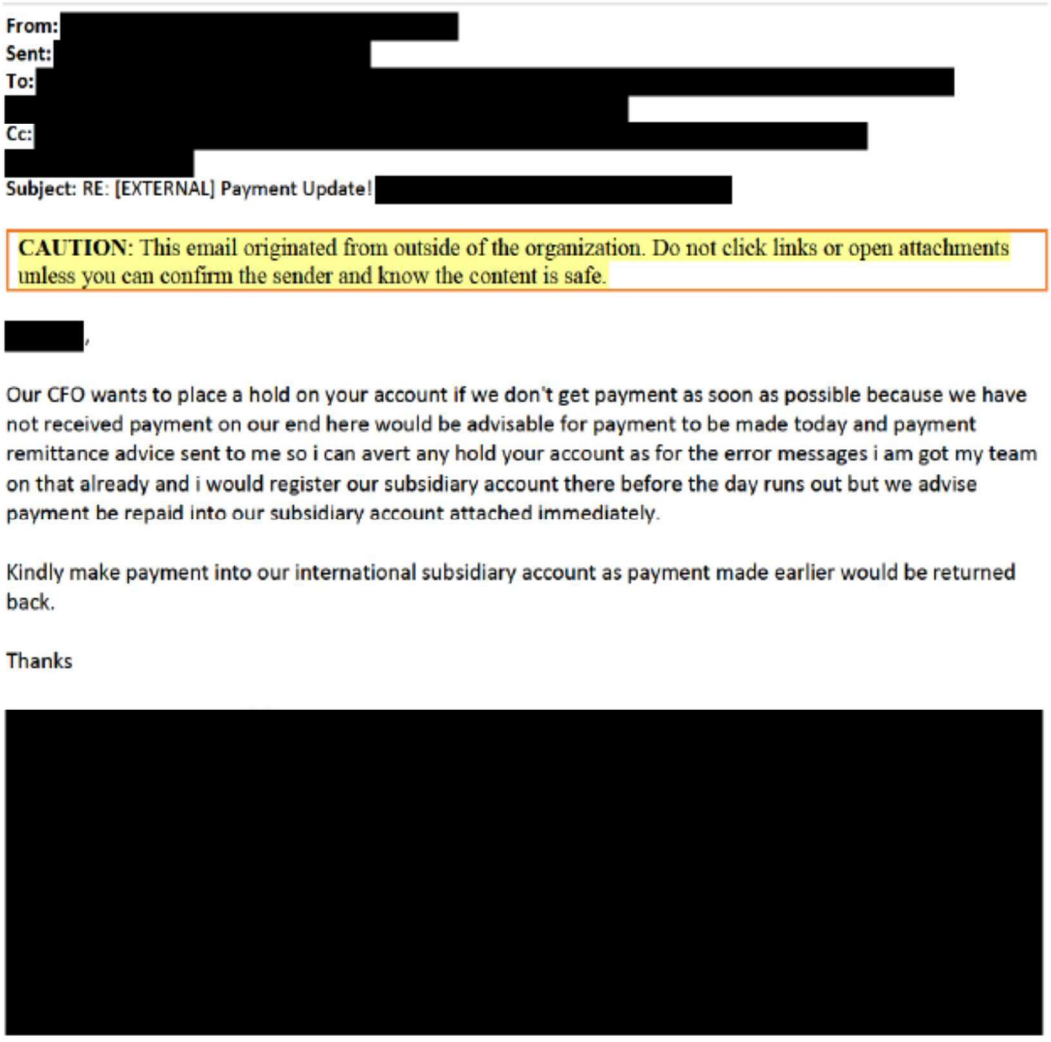
[redacted]

**Figure 1**

35. Defendants capitalized on this opportunity and sent an impersonation email from a homoglyph imposter domain using the *same sender name* and *nearly identical domain*. The only difference between the genuine communication and the imposter communication was a single letter changed in the mail exchange domain – changing sliao.ca to sllao.ca – done to escape notice of the recipient and deceive them into believing the email was a legitimate communication from a known trusted source.

36. Defendants used the same subject line and format of an email from the earlier, legitimate

conversation, but falsely claimed a hold was placed on the account by the CFO, time was running out, and payment needed to be received as soon as possible:


From: [redacted]
Sent: [redacted]
To: [redacted]
Cc: [redacted]
Subject: RE: [EXTERNAL] Payment Update! [redacted]

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you can confirm the sender and know the content is safe.

[redacted],

Our CFO wants to place a hold on your account if we don't get payment as soon as possible because we have not received payment on our end here would be advisable for payment to be made today and payment remittance advice sent to me so i can avert any hold your account as for the error messages i am got my team on that already and i would register our subsidiary account there before the day runs out but we advise payment be repaid into our subsidiary account attached immediately.

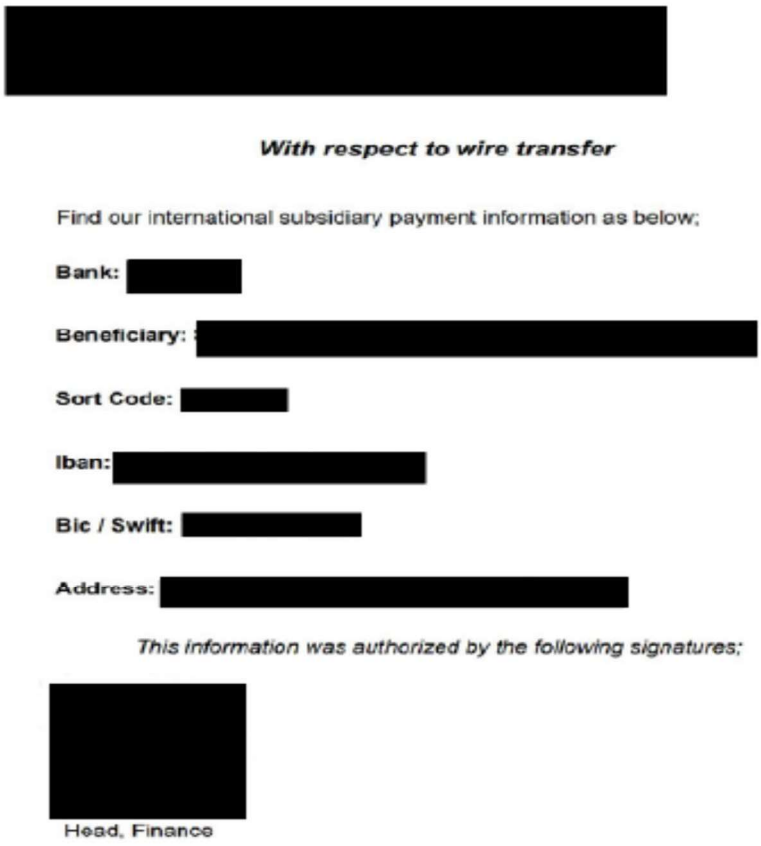
Kindly make payment into our international subsidiary account as payment made earlier would be returned back.

Thanks

[redacted]

**Figure 2**

37. Defendants then solicit a fraudulent wire transfer by sending new wire transfer information appearing to be legitimate and including company logo information, requesting funds be sent to Defendants:


[redacted]

*With respect to wire transfer*

Find our international subsidiary payment information as below;

**Bank:** [redacted]

**Beneficiary:** [redacted]

**Sort Code:** [redacted]

**Iban:** [redacted]

**Bic / Swift:** [redacted]

**Address:** [redacted]

*This information was authorized by the following signatures;*

[redacted]

Head, Finance

**Figure 3**

38. Defendants do not rely on malicious links or attachments in these communications – instead using the intelligence needed to imitate legitimate business transactions gathered after unlawfully accessing a compromised account– in an effort to evade detection and which makes it more difficult to identify malicious emails.

39. Defendants' tactics are more effective because financial fraud victims (either as part of the compromised O365 account victim's business or their larger network) are familiar with the legitimate name of the impersonated email sender as well as the genuine domain name that the homoglyph imposter domain name impersonates, all of which make it less likely the victim will suspect malicious activity.

40. Defendants' conduct is fraudulent and deceptive and designed to be resilient

through the use of homoglyph imposter domains registered via third-party domain providers that can be ported to any infrastructure under the Defendants' control, including outside the O365 environment, impeding Microsoft's ability to protect customers and prevent further attacks once homoglyph imposter domains are ported to third-party infrastructure.

41. Defendants are aware that their conduct violates Microsoft's terms and conditions and is against the law. As a result, once detected or addressed by Microsoft through technical tools at its disposal, Defendants will often move their malicious infrastructure (and domains) outside the Microsoft ecosystem in an attempt to continue their illegal activities, or register and host domains wholly outside Microsoft's ecosystem from the outset.

## V. DEFENDANTS REGISTER HOMOGLYPH IMPOSTER DOMAIN NAMES TO IMPERSONATE DOMAINS OF LEGITIMATE MICROSOFT CUSTOMERS

42. As discussed, Defendants have registered numerous homoglyph imposter domain names (and created numerous imitation email accounts under these domains) in furtherance of their illegal activities. The following are domain names that Defendants are currently leveraging in their infrastructure, which includes .COM top-level domains (TLD) operated by Verisign as the Internet Corporation for Assigned Names and Numbers (ICANN) accredited registry within the Eastern District of Virginia.

43. Defendants registered multiple homoglyph imposter domains listed below including the one used above in soliciting a fraudulent wire transfer:

| **Homoglyph Imposter Domains** | **Registrar** |
|---|---|
| ccp-edu.com | NameSilo, LLC |
| junctionfuelings.com | NameSilo, LLC |
| lverk.com | NameSilo, LLC |
| tattersails.com | NameSilo, LLC |
| cupidoconstructlon.com | NameSilo, LLC |
| thegiaint.com | NameSilo, LLC |
| leaseacceierator.com | NameSilo, LLC |

| | |
|---|---|
| kimballlnternational.com | NameSilo, LLC |
| nationalsafetyconsuiting.com | NameSilo, LLC |
| ldisuperstore.com | NameSilo, LLC |
| lithlumamericas.com | NameSilo, LLC |
| usgeomatlcs.com | NameSilo, LLC |
| ldimn.com | NameSilo, LLC |
| aerocerts.com | NameSilo, LLC |
| napieslegal.com | NameSilo, LLC |
| sllao.ca | KS Domains Ltd./Key Systems GmbH |
| exarr.co | NameSilo, LLC |

44. These domain names used by Defendants are identified in Appendix A to the Complaint and attached as **Exhibit 1** to this declaration. As part of my investigation, I queried for these domain names in a publicly accessible "WHOIS" database, which contains available contact information regarding the registrants of these domain names, domain name registrars, and domain name web host. Information in Exhibit 1 is generated from the publicly available WHOIS registration data. Exhibit 1 includes, for each domain name, the available public contact information for Defendants and contact information for the relevant third-party domain registries, as well as the contact for the relevant domain registrars.

## VI. DEFENDANTS ATTACKED MANY MICROSOFT CUSTOMERS IN THE EASTERN DISTRICT OF VIRGINIA AND AROUND THE WORLD

45. Through my investigation, I determined that Defendants affirmatively targeted Microsoft customers in Virginia, including the Eastern District of Virginia, and throughout the United States and the world.

46. In addition, Defendants registered homoglyph imposter domains through domain registries located in the Eastern District of Virginia.

## VII. HARM TO MICROSOFT

47. Microsoft® is a provider of the Office 365® cloud-based business and productivity

suite of services. Microsoft has invested substantial resources in developing and marketing resilient and secure cloud services. Due to the security and effectiveness of Microsoft's services, Microsoft has generated substantial trust with its customers to protect their data, has established a strong brand as a leader in the security market, and has developed the Microsoft name and the names of its services into famous world-wide symbols that are well-recognized within its channels of trade.

48. Defendants have obtained login credentials stolen from Microsoft customers and unlawfully used those credentials to gain unauthorized access to Office 365 accounts in an effort to identify potential victims and opportunities to fraudulently solicit wire transfers. Defendants register homoglyph imposter domains, host those domains on fraudulently procured O365 tenants, and establish impersonation email addresses in an effort to insert themselves into legitimate business conversations and deceive recipients – either O365 customers or members of their trusted networks including those using other email accounts – into transferring funds to Defendants.

49. Once identified, Microsoft can disable access to fraudulent O365 tenants and accounts. However, even once Defendants lose access to the compromised O365 tenant, Defendants still own the homoglyph imposter domain names they registered and can move those domains to other domain registrars and hosting facilities, where they can set up new email accounts on the domains outside of Microsoft's ecosystem, and then use those domains and associated emails to continue their attacks on Microsoft, Microsoft customers and their trusted networks. Alternatively, Defendants can also register domains and host those domains from the outset through third party domain registrars and hosting facilities beyond Microsoft's control.

50. In essence, after registering the homoglyph imposter domains, Defendants have

portable, weaponized mail exchange domains that can be associated to any email service provider and then used in the future to attack Microsoft customers. The threat is ongoing and pervasive, since Defendants now have the necessary tools, information, and capability to perpetrate further attacks.

51. All of these activities cause injury to Microsoft. Customers expect Microsoft to provide safe and trustworthy products and services. There is a great risk that Microsoft's customers may incorrectly attribute Defendants' malicious activities to Microsoft's products and services. Further, Defendants' ability to damage Microsoft's reputation extends even after they are detected and lose access to O365 since they can take their weaponized domains to other platforms and continue attacks. Victims of Defendants' malicious attacks may incorrectly believe that Microsoft is the source of problems, harming customer relationships, or devaluing O365 as a platform, which further causes reputational injury to Microsoft – all because of Defendants' malicious activity and financial fraud.

52. Microsoft is similarly injured because Defendants attempt to launch their scheme from within Microsoft's Office 365 service in an effort to victimize Microsoft customers. Microsoft must bear an extraordinary burden to address cybercrime directed at its services and customers. Microsoft must develop technical countermeasures and defenses, to suppress Defendants' activities, address customer service issues caused by Defendants and must expend substantial resources dealing with the injury and confusion and to resist ongoing attempted attacks on its infrastructure, products, services, and customers. Given that Defendants continue to target Microsoft and its customers, and that such attacks will be ongoing, this poses severe risk of injury to Microsoft, threatening Microsoft's brands and customer relationships.

53. Based on my experience assessing cybercrime threats and the impact on business,

I conclude that customers may incorrectly attribute the negative impact of Defendants' activity to Microsoft. Further, based on my experience, I therefore conclude that if permitted to continue unabated, there is a serious risk that Defendants may interfere with Microsoft's customer relationships.

## VIII. DISABLING DEFENDANTS' ABILITY TO USE THE HOMOGLYPH IMPOSTER DOMAINS IS THE ONLY WAY TO PREVENT ONGOING INJURY

54. Evidence indicates that Defendants are persistent, sophisticated, pose an immediate risk and are determined to attempt to overcome Microsoft's technical and other mitigation steps to date.

55. Microsoft requests that the domain registrars located in the United States place the malicious domains identified in **Exhibit 1** to this Declaration on client hold status to prevent the domains from resolving in the domain name system, on client transfer prohibited status to prevent the domains from being transferred, on client update status to prevent the domains from being updated by Defendants, and otherwise taking all steps to prevent Defendants from accessing, modifying, transferring or using in any manner the malicious homoglyph domains until the expiration of the domains at the end of the current registration period to prevent further malicious activity and mitigate risk and injury to Microsoft and its customers.

56. Further, Microsoft requests that the domain registries located in the United States place the domains on server transfer prohibited status to prevent the domains from being transferred to a different registrar until the expiration of the domains at the end of the current registration period.

57. Based on my prior experience with similar operations and malicious technical infrastructure, I conclude that the only way to suspend the injury caused to Microsoft, its customers, and the public, is to take the steps described in the Proposed Ex Parte Temporary

Restraining Order and Order to Show Cause Re Preliminary Injunction ("Proposed TRO"). This relief will significantly hinder Defendants' ability to use the weaponized domains to solicit further financially fraudulent transactions using intelligence gathered on the networks of compromised O365 account users and to further target O365 account users and others for financial fraud. In the absence of such action, Defendants will be able to continue using these homoglyph imposter domains to target new victims to Defendants.

58. Defendants' techniques are designed to resist technical mitigation efforts, eliminating straightforward technical means to curb the injury being caused. Even if they are detected and Microsoft eliminates Defendants' access to O365 services, Defendants have the ability to move these weaponized homoglyph imposter domains outside the O365 network and continue attacks.

59. For this reason, providing notice to Defendants in advance of placing the homoglyph imposter domain names on client hold status and transfer prohibited status would render attempts to disable the infrastructure futile. Further, when 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. Based on my experience observing the operation of numerous threat actors such as Defendants, I believe Defendants would attempt to conceal the extent of their operations and continue to victimize Microsoft, its customers, and their networks and defend their infrastructure, if they were to learn of Microsoft's impending action and request for relief.

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 12th day of July, 2021, in Seattle WA.

Donal Keating

**EXHIBIT 1**

| **.COM DOMAINS**<br><br>***Registrar***<br>**NameSilo LLC**<br>**8825 N. 23rd Ave Suite 100**<br>**Phoenix, AZ 85021**<br>**United States** | |
|---|---|
| ccp-edu.com | Domain Name: ccp-edu.com<br>Registry Domain ID: 2587672139_DOMAIN_COM-VRSN<br>Registrar WHOIS Server: whois.namesilo.com<br>Registrar URL: https://www.namesilo.com/<br>Updated Date: 2021-02-24T07:00:00Z<br>Creation Date: 2021-01-28T07:00:00Z<br>Registrar Registration Expiration Date: 2022-01-28T07:00:00Z<br>Registrar: NameSilo, LLC<br>Registrar IANA ID: 1479<br>Registrar Abuse Contact Email: abuse@namesilo.com<br>Registrar Abuse Contact Phone: +1.4805240066<br>Reseller: QHOSTER.COM<br>Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited<br>Registry Registrant ID:<br>Registrant Name: Robert Chris<br>Registrant Organization:<br>Registrant Street: 3126 Tea Berry Lane<br>Registrant City: Eau Claire<br>Registrant State/Province: WI<br>Registrant Postal Code: 54701<br>Registrant Country: US<br>Registrant Phone: +1.5185025850<br>Registrant Phone Ext:<br>Registrant Fax:<br>Registrant Fax Ext:<br>Registrant Email: zohoferdz1@gmail.com<br>Registry Admin ID:<br>Admin Name: Robert Chris<br>Admin Organization:<br>Admin Street: 3126 Tea Berry Lane<br>Admin City: Eau Claire<br>Admin State/Province: WI<br>Admin Postal Code: 54701<br>Admin Country: US |

| | |
|---|---|
| | Admin Phone: +1.5185025850<br>Admin Phone Ext:<br>Admin Fax:<br>Admin Fax Ext:<br>Admin Email: zohoferdz1@gmail.com<br>Registry Tech ID:<br>Tech Name: Robert Chris<br>Tech Organization:<br>Tech Street: 3126 Tea Berry Lane<br>Tech City: Eau Claire<br>Tech State/Province: WI<br>Tech Postal Code: 54701<br>Tech Country: US<br>Tech Phone: +1.5185025850<br>Tech Phone Ext:<br>Tech Fax:<br>Tech Fax Ext:<br>Tech Email: zohoferdz1@gmail.com<br>Name Server: NS73.DOMAINCONTROL.COM<br>Name Server: NS74.DOMAINCONTROL.COM<br>DNSSEC: unsigned |
| junctionfuelings.com | Domain Name: junctionfuelings.com<br>Registry Domain ID: 2588515748_DOMAIN_COM-VRSN<br>Registrar WHOIS Server: whois.namesilo.com<br>Registrar URL: https://www.namesilo.com/<br>http://www.namesilo.com<br>Updated Date: 2021-02-01T07:00:00+00:00<br>2021-02-01<br>Creation Date: 2021-02-01T07:00:00+00:00<br>2021-02-01<br>Registrar Registration Expiration Date: 2022-02-01T07:00:00+00:00<br>2022-02-01<br>Registrar: NameSilo, LLC<br>Sponsoring Registrar IANA ID: 1479<br>Registrar Abuse Contact Email: abuse@namesilo.com<br>Registrar Abuse Contact Phone: 14805240066<br>Status:<br>clientTransferProhibited<br>Registry Registrant ID:<br>Registrant Name: REDACTED FOR PRIVACY (DT)<br>Registrant Organization:<br>Registrant Street: REDACTED FOR PRIVACY (DT)<br>Registrant City: REDACTED FOR PRIVACY (DT)<br>Registrant State/Province: CA<br>Registrant Postal Code: REDACTED FOR PRIVACY (DT)<br>Registrant Country: us<br>Registrant Phone: REDACTED FOR PRIVACY (DT)<br>Registrant Phone Ext: |

| | |
|---|---|
| | Registrant Fax:<br>Registrant Fax Ext:<br>Registrant Email: REDACTED FOR PRIVACY (DT)<br>Registry Admin ID:<br>Admin Name: REDACTED FOR PRIVACY (DT)<br>Admin Organization:<br>Admin Street: REDACTED FOR PRIVACY (DT)<br>Admin City: REDACTED FOR PRIVACY (DT)<br>Admin State/Province: CA<br>Admin Postal Code: REDACTED FOR PRIVACY (DT)<br>Admin Country: us<br>Admin Phone: REDACTED FOR PRIVACY (DT)<br>Admin Phone Ext:<br>Admin Fax:<br>Admin Fax Ext:<br>Admin Email: REDACTED FOR PRIVACY (DT)<br>Registry Tech ID:<br>Tech Name: REDACTED FOR PRIVACY (DT)<br>Tech Organization:<br>Tech Street: REDACTED FOR PRIVACY (DT)<br>Tech City: REDACTED FOR PRIVACY (DT)<br>Tech State/Province: CA<br>Tech Postal Code: REDACTED FOR PRIVACY (DT)<br>Tech Country: us<br>Tech Phone: REDACTED FOR PRIVACY (DT)<br>Tech Phone Ext:<br>Tech Fax:<br>Tech Fax Ext:<br>Tech Email: REDACTED FOR PRIVACY (DT)<br>Registry Billing ID:<br>Billing Name:<br>Billing Organization:<br>Billing Street:<br>Billing City:<br>Billing State/Province:<br>Billing Postal Code:<br>Billing Country:<br>Billing Phone:<br>Billing Phone Ext:<br>Billing Fax:<br>Billing Fax Ext:<br>Billing Email:<br>Nameservers:<br>ns07.domaincontrol.com<br>ns08.domaincontrol.com<br>Reseller: QHOSTER.COM<br>DNSSEC: unsigned |
| lverk.com | Domain Name: lverk.com<br>Registry Domain ID: 2588449215_DOMAIN_COM-VRSN |

| | |
|---|---|
| | Registrar WHOIS Server: whois.namesilo.com<br>Registrar URL: https://www.namesilo.com/<br>Updated Date: 2021-02-24T07:00:00Z<br>Creation Date: 2021-02-01T07:00:00Z<br>Registrar Registration Expiration Date: 2022-02-01T07:00:00Z<br>Registrar: NameSilo, LLC<br>Registrar IANA ID: 1479<br>Registrar Abuse Contact Email: abuse@namesilo.com<br>Registrar Abuse Contact Phone: +1.4805240066<br>Reseller: QHOSTER.COM<br>Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited<br>Registry Registrant ID:<br>Registrant Name: Robert Chris<br>Registrant Organization:<br>Registrant Street: 3126 Tea Berry Lane<br>Registrant City: Eau Claire<br>Registrant State/Province: WI<br>Registrant Postal Code: 54701<br>Registrant Country: US<br>Registrant Phone: +1.5185025850<br>Registrant Phone Ext:<br>Registrant Fax:<br>Registrant Fax Ext:<br>Registrant Email: zohoferdz1@gmail.com<br>Registry Admin ID:<br>Admin Name: Robert Chris<br>Admin Organization:<br>Admin Street: 3126 Tea Berry Lane<br>Admin City: Eau Claire<br>Admin State/Province: WI<br>Admin Postal Code: 54701<br>Admin Country: US<br>Admin Phone: +1.5185025850<br>Admin Phone Ext:<br>Admin Fax:<br>Admin Fax Ext:<br>Admin Email: zohoferdz1@gmail.com<br>Registry Tech ID:<br>Tech Name: Robert Chris<br>Tech Organization:<br>Tech Street: 3126 Tea Berry Lane<br>Tech City: Eau Claire<br>Tech State/Province: WI<br>Tech Postal Code: 54701<br>Tech Country: US<br>Tech Phone: +1.5185025850<br>Tech Phone Ext:<br>Tech Fax:<br>Tech Fax Ext: |

| | |
|---|---|
| | Tech Email: zohoferdz1@gmail.com<br>Name Server: NS17.DOMAINCONTROL.COM<br>Name Server: NS18.DOMAINCONTROL.COM<br>DNSSEC: unsigned |
| tattersails.com | omain Name: tattersails.com<br>Registry Domain ID: 2588455590_DOMAIN_COM-VRSN<br>Registrar WHOIS Server: whois.namesilo.com<br>Registrar URL: https://www.namesilo.com/<br>Updated Date: 2021-02-24T07:00:00Z<br>Creation Date: 2021-02-01T07:00:00Z<br>Registrar Registration Expiration Date: 2022-02-01T07:00:00Z<br>Registrar: NameSilo, LLC<br>Registrar IANA ID: 1479<br>Registrar Abuse Contact Email: abuse@namesilo.com<br>Registrar Abuse Contact Phone: +1.4805240066<br>Reseller: QHOSTER.COM<br>Domain Status: clientTransferProhibited<br>https://www.icann.org/epp#clientTransferProhibited<br>Registry Registrant ID:<br>Registrant Name: Robert Chris<br>Registrant Organization:<br>Registrant Street: 3126 Tea Berry Lane<br>Registrant City: Eau Claire<br>Registrant State/Province: WI<br>Registrant Postal Code: 54701<br>Registrant Country: US<br>Registrant Phone: +1.5185025850<br>Registrant Phone Ext:<br>Registrant Fax:<br>Registrant Fax Ext:<br>Registrant Email: zohoferdz1@gmail.com<br>Registry Admin ID:<br>Admin Name: Robert Chris<br>Admin Organization:<br>Admin Street: 3126 Tea Berry Lane<br>Admin City: Eau Claire<br>Admin State/Province: WI<br>Admin Postal Code: 54701<br>Admin Country: US<br>Admin Phone: +1.5185025850<br>Admin Phone Ext:<br>Admin Fax:<br>Admin Fax Ext:<br>Admin Email: zohoferdz1@gmail.com<br>Registry Tech ID:<br>Tech Name: Robert Chris<br>Tech Organization:<br>Tech Street: 3126 Tea Berry Lane<br>Tech City: Eau Claire |

| | |
|---|---|
| | Tech State/Province: WI<br>Tech Postal Code: 54701<br>Tech Country: US<br>Tech Phone: +1.5185025850<br>Tech Phone Ext:<br>Tech Fax:<br>Tech Fax Ext:<br>Tech Email: zohoferdz1@gmail.com<br>Name Server: NS29.DOMAINCONTROL.COM<br>Name Server: NS30.DOMAINCONTROL.COM<br>DNSSEC: unsigned |
| cupidoconstructlon.com | Domain Name: cupidoconstructlon.com<br>Registry Domain ID: 2588516962_DOMAIN_COM-VRSN<br>Registrar WHOIS Server: whois.namesilo.com<br>Registrar URL: https://www.namesilo.com/<br>Updated Date: 2021-02-24T07:00:00Z<br>Creation Date: 2021-02-01T07:00:00Z<br>Registrar Registration Expiration Date: 2022-02-01T07:00:00Z<br>Registrar: NameSilo, LLC<br>Registrar IANA ID: 1479<br>Registrar Abuse Contact Email: abuse@namesilo.com<br>Registrar Abuse Contact Phone: +1.4805240066<br>Reseller: QHOSTER.COM<br>Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited<br>Registry Registrant ID:<br>Registrant Name: Robert Chris<br>Registrant Organization:<br>Registrant Street: 3126 Tea Berry Lane<br>Registrant City: Eau Claire<br>Registrant State/Province: WI<br>Registrant Postal Code: 54701<br>Registrant Country: US<br>Registrant Phone: +1.5185025850<br>Registrant Phone Ext:<br>Registrant Fax:<br>Registrant Fax Ext:<br>Registrant Email: zohoferdz1@gmail.com<br>Registry Admin ID:<br>Admin Name: Robert Chris<br>Admin Organization:<br>Admin Street: 3126 Tea Berry Lane<br>Admin City: Eau Claire<br>Admin State/Province: WI<br>Admin Postal Code: 54701<br>Admin Country: US<br>Admin Phone: +1.5185025850<br>Admin Phone Ext:<br>Admin Fax: |

| | |
|---|---|
| | Admin Fax Ext:<br>Admin Email: zohoferdz1@gmail.com<br>Registry Tech ID:<br>Tech Name: Robert Chris<br>Tech Organization:<br>Tech Street: 3126 Tea Berry Lane<br>Tech City: Eau Claire<br>Tech State/Province: WI<br>Tech Postal Code: 54701<br>Tech Country: US<br>Tech Phone: +1.5185025850<br>Tech Phone Ext:<br>Tech Fax:<br>Tech Fax Ext:<br>Tech Email: zohoferdz1@gmail.com<br>Name Server: NS51.DOMAINCONTROL.COM<br>Name Server: NS52.DOMAINCONTROL.COM<br>DNSSEC: unsigned |
| thegiaint.com | Domain Name: thegiaint.com<br>Registry Domain ID: 2589038736_DOMAIN_COM-VRSN<br>Registrar WHOIS Server: whois.namesilo.com<br>Registrar URL: https://www.namesilo.com/<br>http://www.namesilo.com<br>Updated Date: 2021-02-04T07:00:00+00:00<br>2021-02-03<br>Creation Date: 2021-02-03T07:00:00+00:00<br>2021-02-03<br>Registrar Registration Expiration Date: 2022-02-03T07:00:00+00:00<br>2022-02-03<br>Registrar: NameSilo, LLC<br>Sponsoring Registrar IANA ID: 1479<br>Registrar Abuse Contact Email: abuse@namesilo.com<br>Registrar Abuse Contact Phone: 14805240066<br>Status:<br>clientTransferProhibited<br>Registry Registrant ID:<br>Registrant Name: REDACTED FOR PRIVACY (DT)<br>Registrant Organization:<br>Registrant Street: REDACTED FOR PRIVACY (DT)<br>Registrant City: REDACTED FOR PRIVACY (DT)<br>Registrant State/Province: CA<br>Registrant Postal Code: REDACTED FOR PRIVACY (DT)<br>Registrant Country: us<br>Registrant Phone: REDACTED FOR PRIVACY (DT)<br>Registrant Phone Ext:<br>Registrant Fax:<br>Registrant Fax Ext:<br>Registrant Email: REDACTED FOR PRIVACY (DT) |

| | |
|---|---|
| | Registry Admin ID:<br>Admin Name: REDACTED FOR PRIVACY (DT)<br>Admin Organization:<br>Admin Street: REDACTED FOR PRIVACY (DT)<br>Admin City: REDACTED FOR PRIVACY (DT)<br>Admin State/Province: CA<br>Admin Postal Code: REDACTED FOR PRIVACY (DT)<br>Admin Country: us<br>Admin Phone: REDACTED FOR PRIVACY (DT)<br>Admin Phone Ext:<br>Admin Fax:<br>Admin Fax Ext:<br>Admin Email: REDACTED FOR PRIVACY (DT)<br>Registry Tech ID:<br>Tech Name: REDACTED FOR PRIVACY (DT)<br>Tech Organization:<br>Tech Street: REDACTED FOR PRIVACY (DT)<br>Tech City: REDACTED FOR PRIVACY (DT)<br>Tech State/Province: CA<br>Tech Postal Code: REDACTED FOR PRIVACY (DT)<br>Tech Country: us<br>Tech Phone: REDACTED FOR PRIVACY (DT)<br>Tech Phone Ext:<br>Tech Fax:<br>Tech Fax Ext:<br>Tech Email: REDACTED FOR PRIVACY (DT)<br>Registry Billing ID:<br>Billing Name:<br>Billing Organization:<br>Billing Street:<br>Billing City:<br>Billing State/Province:<br>Billing Postal Code:<br>Billing Country:<br>Billing Phone:<br>Billing Phone Ext:<br>Billing Fax:<br>Billing Fax Ext:<br>Billing Email:<br>Nameservers:<br>ns51.domaincontrol.com<br>ns52.domaincontrol.com<br>Reseller: QHOSTER.COM<br>DNSSEC: unsigned |
| leaseacceierator.com | Domain Name: leaseacceierator.com<br>Registry Domain ID: 2589022048_DOMAIN_COM-VRSN<br>Registrar WHOIS Server: whois.namesilo.com<br>Registrar URL: https://www.namesilo.com/<br>Updated Date: 2021-02-24T07:00:00Z<br>Creation Date: 2021-02-03T07:00:00Z |

| | |
|---|---|
| | Registrar Registration Expiration Date: 2022-02-03T07:00:00Z<br>Registrar: NameSilo, LLC<br>Registrar IANA ID: 1479<br>Registrar Abuse Contact Email: abuse@namesilo.com<br>Registrar Abuse Contact Phone: +1.4805240066<br>Reseller: QHOSTER.COM<br>Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited<br>Registry Registrant ID:<br>Registrant Name: Robert Chris<br>Registrant Organization:<br>Registrant Street: 3126 Tea Berry Lane<br>Registrant City: Eau Claire<br>Registrant State/Province: WI<br>Registrant Postal Code: 54701<br>Registrant Country: US<br>Registrant Phone: +1.5185025850<br>Registrant Phone Ext:<br>Registrant Fax:<br>Registrant Fax Ext:<br>Registrant Email: zohoferdz1@gmail.com<br>Registry Admin ID:<br>Admin Name: Robert Chris<br>Admin Organization:<br>Admin Street: 3126 Tea Berry Lane<br>Admin City: Eau Claire<br>Admin State/Province: WI<br>Admin Postal Code: 54701<br>Admin Country: US<br>Admin Phone: +1.5185025850<br>Admin Phone Ext:<br>Admin Fax:<br>Admin Fax Ext:<br>Admin Email: zohoferdz1@gmail.com<br>Registry Tech ID:<br>Tech Name: Robert Chris<br>Tech Organization:<br>Tech Street: 3126 Tea Berry Lane<br>Tech City: Eau Claire<br>Tech State/Province: WI<br>Tech Postal Code: 54701<br>Tech Country: US<br>Tech Phone: +1.5185025850<br>Tech Phone Ext:<br>Tech Fax:<br>Tech Fax Ext:<br>Tech Email: zohoferdz1@gmail.com<br>Name Server: NS23.DOMAINCONTROL.COM<br>Name Server: NS24.DOMAINCONTROL.COM<br>DNSSEC: unsigned |

| | |
|---|---|
| kimballlnternational.com | Domain Name: kimballlnternational.com<br>Registry Domain ID: 2589075541_DOMAIN_COM-VRSN<br>Registrar WHOIS Server: whois.namesilo.com<br>Registrar URL: https://www.namesilo.com/<br>Updated Date: 2021-02-24T07:00:00Z<br>Creation Date: 2021-02-03T07:00:00Z<br>Registrar Registration Expiration Date: 2022-02-03T07:00:00Z<br>Registrar: NameSilo, LLC<br>Registrar IANA ID: 1479<br>Registrar Abuse Contact Email: abuse@namesilo.com<br>Registrar Abuse Contact Phone: +1.4805240066<br>Reseller: QHOSTER.COM<br>Domain Status: clientTransferProhibited<br>https://www.icann.org/epp#clientTransferProhibited<br>Registry Registrant ID:<br>Registrant Name: Robert Chris<br>Registrant Organization:<br>Registrant Street: 3126 Tea Berry Lane<br>Registrant City: Eau Claire<br>Registrant State/Province: WI<br>Registrant Postal Code: 54701<br>Registrant Country: US<br>Registrant Phone: +1.5185025850<br>Registrant Phone Ext:<br>Registrant Fax:<br>Registrant Fax Ext:<br>Registrant Email: zohoferdz1@gmail.com<br>Registry Admin ID:<br>Admin Name: Robert Chris<br>Admin Organization:<br>Admin Street: 3126 Tea Berry Lane<br>Admin City: Eau Claire<br>Admin State/Province: WI<br>Admin Postal Code: 54701<br>Admin Country: US<br>Admin Phone: +1.5185025850<br>Admin Phone Ext:<br>Admin Fax:<br>Admin Fax Ext:<br>Admin Email: zohoferdz1@gmail.com<br>Registry Tech ID:<br>Tech Name: Robert Chris<br>Tech Organization:<br>Tech Street: 3126 Tea Berry Lane<br>Tech City: Eau Claire<br>Tech State/Province: WI<br>Tech Postal Code: 54701<br>Tech Country: US<br>Tech Phone: +1.5185025850 |

| | |
|---|---|
| | Tech Phone Ext:<br>Tech Fax:<br>Tech Fax Ext:<br>Tech Email: zohoferdz1@gmail.com<br>Name Server: NS37.DOMAINCONTROL.COM<br>Name Server: NS38.DOMAINCONTROL.COM<br>DNSSEC: unsigned |
| nationalsafetyconsuiting.com | Domain Name: nationalsafetyconsuiting.com<br>Registry Domain ID: 2589004393_DOMAIN_COM-VRSN<br>Registrar WHOIS Server: whois.namesilo.com<br>Registrar URL: https://www.namesilo.com/<br>http://www.namesilo.com<br>Updated Date: 2021-02-04T07:00:00+00:00<br>2021-02-03<br>Creation Date: 2021-02-03T07:00:00+00:00<br>2021-02-03<br>Registrar Registration Expiration Date: 2022-02-03T07:00:00+00:00<br>2022-02-03<br>Registrar: NameSilo, LLC<br>Sponsoring Registrar IANA ID: 1479<br>Registrar Abuse Contact Email: abuse@namesilo.com<br>Registrar Abuse Contact Phone: 14805240066<br>Status:<br>clientTransferProhibited<br>Registry Registrant ID:<br>Registrant Name: REDACTED FOR PRIVACY (DT)<br>Registrant Organization:<br>Registrant Street: REDACTED FOR PRIVACY (DT)<br>Registrant City: REDACTED FOR PRIVACY (DT)<br>Registrant State/Province: CA<br>Registrant Postal Code: REDACTED FOR PRIVACY (DT)<br>Registrant Country: us<br>Registrant Phone: REDACTED FOR PRIVACY (DT)<br>Registrant Phone Ext:<br>Registrant Fax:<br>Registrant Fax Ext:<br>Registrant Email: REDACTED FOR PRIVACY (DT)<br>Registry Admin ID:<br>Admin Name: REDACTED FOR PRIVACY (DT)<br>Admin Organization:<br>Admin Street: REDACTED FOR PRIVACY (DT)<br>Admin City: REDACTED FOR PRIVACY (DT)<br>Admin State/Province: CA<br>Admin Postal Code: REDACTED FOR PRIVACY (DT)<br>Admin Country: us<br>Admin Phone: REDACTED FOR PRIVACY (DT)<br>Admin Phone Ext:<br>Admin Fax: |

| | |
|---|---|
| | Admin Fax Ext:<br>Admin Email: REDACTED FOR PRIVACY (DT)<br>Registry Tech ID:<br>Tech Name: REDACTED FOR PRIVACY (DT)<br>Tech Organization:<br>Tech Street: REDACTED FOR PRIVACY (DT)<br>Tech City: REDACTED FOR PRIVACY (DT)<br>Tech State/Province: CA<br>Tech Postal Code: REDACTED FOR PRIVACY (DT)<br>Tech Country: us<br>Tech Phone: REDACTED FOR PRIVACY (DT)<br>Tech Phone Ext:<br>Tech Fax:<br>Tech Fax Ext:<br>Tech Email: REDACTED FOR PRIVACY (DT)<br>Registry Billing ID:<br>Billing Name:<br>Billing Organization:<br>Billing Street:<br>Billing City:<br>Billing State/Province:<br>Billing Postal Code:<br>Billing Country:<br>Billing Phone:<br>Billing Phone Ext:<br>Billing Fax:<br>Billing Fax Ext:<br>Billing Email:<br>Nameservers:<br>ns57.domaincontrol.com<br>ns58.domaincontrol.com<br>Reseller: QHOSTER.COM<br>DNSSEC: unsigned |
| ldisuperstore.com | Domain Name: ldisuperstore.com<br>Registry Domain ID: 2589471467_DOMAIN_COM-VRSN<br>Registrar WHOIS Server: whois.namesilo.com<br>Registrar URL: https://www.namesilo.com/<br>Updated Date: 2021-02-24T07:00:00Z<br>Creation Date: 2021-02-05T07:00:00Z<br>Registrar Registration Expiration Date: 2022-02-05T07:00:00Z<br>Registrar: NameSilo, LLC<br>Registrar IANA ID: 1479<br>Registrar Abuse Contact Email: abuse@namesilo.com<br>Registrar Abuse Contact Phone: +1.4805240066<br>Reseller: QHOSTER.COM<br>Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited<br>Registry Registrant ID:<br>Registrant Name: Robert Chris |

| | |
|---|---|
| | Registrant Organization:<br>Registrant Street: 3126 Tea Berry Lane<br>Registrant City: Eau Claire<br>Registrant State/Province: WI<br>Registrant Postal Code: 54701<br>Registrant Country: US<br>Registrant Phone: +1.5185025850<br>Registrant Phone Ext:<br>Registrant Fax:<br>Registrant Fax Ext:<br>Registrant Email: zohoferdz1@gmail.com<br>Registry Admin ID:<br>Admin Name: Robert Chris<br>Admin Organization:<br>Admin Street: 3126 Tea Berry Lane<br>Admin City: Eau Claire<br>Admin State/Province: WI<br>Admin Postal Code: 54701<br>Admin Country: US<br>Admin Phone: +1.5185025850<br>Admin Phone Ext:<br>Admin Fax:<br>Admin Fax Ext:<br>Admin Email: zohoferdz1@gmail.com<br>Registry Tech ID:<br>Tech Name: Robert Chris<br>Tech Organization:<br>Tech Street: 3126 Tea Berry Lane<br>Tech City: Eau Claire<br>Tech State/Province: WI<br>Tech Postal Code: 54701<br>Tech Country: US<br>Tech Phone: +1.5185025850<br>Tech Phone Ext:<br>Tech Fax:<br>Tech Fax Ext:<br>Tech Email: zohoferdz1@gmail.com<br>Name Server: NS75.DOMAINCONTROL.COM<br>Name Server: NS76.DOMAINCONTROL.COM<br>DNSSEC: unsigned |
| lithlumamericas.com | Domain Name: lithlumamericas.com<br>Registry Domain ID: 2590340868_DOMAIN_COM-VRSN<br>Registrar WHOIS Server: whois.namesilo.com<br>Registrar URL: https://www.namesilo.com/<br>Updated Date: 2021-02-10T07:00:00Z<br>Creation Date: 2021-02-09T07:00:00Z<br>Registrar Registration Expiration Date: 2022-02-09T07:00:00Z<br>Registrar: NameSilo, LLC<br>Registrar IANA ID: 1479 |

| | |
|---|---|
| | Registrar Abuse Contact Email: abuse@namesilo.com<br>Registrar Abuse Contact Phone: +1.4805240066<br>Reseller: QHOSTER.COM<br>Domain Status: clientTransferProhibited<br>https://www.icann.org/epp#clientTransferProhibited<br>Registry Registrant ID:<br>Registrant Name: Robert Chris<br>Registrant Organization:<br>Registrant Street: 3126 Tea Berry Lane<br>Registrant City: Eau Claire<br>Registrant State/Province: WI<br>Registrant Postal Code: 54701<br>Registrant Country: US<br>Registrant Phone: +1.5185025850<br>Registrant Phone Ext:<br>Registrant Fax:<br>Registrant Fax Ext:<br>Registrant Email: zohoferdz1@gmail.com<br>Registry Admin ID:<br>Admin Name: Robert Chris<br>Admin Organization:<br>Admin Street: 3126 Tea Berry Lane<br>Admin City: Eau Claire<br>Admin State/Province: WI<br>Admin Postal Code: 54701<br>Admin Country: US<br>Admin Phone: +1.5185025850<br>Admin Phone Ext:<br>Admin Fax:<br>Admin Fax Ext:<br>Admin Email: zohoferdz1@gmail.com<br>Registry Tech ID:<br>Tech Name: Robert Chris<br>Tech Organization:<br>Tech Street: 3126 Tea Berry Lane<br>Tech City: Eau Claire<br>Tech State/Province: WI<br>Tech Postal Code: 54701<br>Tech Country: US<br>Tech Phone: +1.5185025850<br>Tech Phone Ext:<br>Tech Fax:<br>Tech Fax Ext:<br>Tech Email: zohoferdz1@gmail.com<br>Name Server: NS07.DOMAINCONTROL.COM<br>Name Server: NS08.DOMAINCONTROL.COM<br>DNSSEC: unsigned |
| usgeomatlcs.com | Domain Name: usgeomatlcs.com<br>Registry Domain ID: 2590212561_DOMAIN_COM-VRSN<br>Registrar WHOIS Server: whois.namesilo.com |

| | |
|---|---|
| | Registrar URL: https://www.namesilo.com/<br>Updated Date: 2021-02-09T07:00:00Z<br>Creation Date: 2021-02-09T07:00:00Z<br>Registrar Registration Expiration Date: 2022-02-09T07:00:00Z<br>Registrar: NameSilo, LLC<br>Registrar IANA ID: 1479<br>Registrar Abuse Contact Email: abuse@namesilo.com<br>Registrar Abuse Contact Phone: +1.4805240066<br>Reseller: QHOSTER.COM<br>Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited<br>Registry Registrant ID:<br>Registrant Name: Robert Chris<br>Registrant Organization:<br>Registrant Street: 3126 Tea Berry Lane<br>Registrant City: Eau Claire<br>Registrant State/Province: WI<br>Registrant Postal Code: 54701<br>Registrant Country: US<br>Registrant Phone: +1.5185025850<br>Registrant Phone Ext:<br>Registrant Fax:<br>Registrant Fax Ext:<br>Registrant Email: zohoferdz1@gmail.com<br>Registry Admin ID:<br>Admin Name: Robert Chris<br>Admin Organization:<br>Admin Street: 3126 Tea Berry Lane<br>Admin City: Eau Claire<br>Admin State/Province: WI<br>Admin Postal Code: 54701<br>Admin Country: US<br>Admin Phone: +1.5185025850<br>Admin Phone Ext:<br>Admin Fax:<br>Admin Fax Ext:<br>Admin Email: zohoferdz1@gmail.com<br>Registry Tech ID:<br>Tech Name: Robert Chris<br>Tech Organization:<br>Tech Street: 3126 Tea Berry Lane<br>Tech City: Eau Claire<br>Tech State/Province: WI<br>Tech Postal Code: 54701<br>Tech Country: US<br>Tech Phone: +1.5185025850<br>Tech Phone Ext:<br>Tech Fax:<br>Tech Fax Ext:<br>Tech Email: zohoferdz1@gmail.com |

| | |
|---|---|
| | Name Server: NS05.DOMAINCONTROL.COM<br>Name Server: NS06.DOMAINCONTROL.COM<br>DNSSEC: unsigned |
| ldimn.com | Domain Name: ldimn.com<br>Registry Domain ID: 2590498945_DOMAIN_COM-VRSN<br>Registrar WHOIS Server: whois.namesilo.com<br>Registrar URL: https://www.namesilo.com/<br>Updated Date: 2021-02-11T07:00:00Z<br>Creation Date: 2021-02-10T07:00:00Z<br>Registrar Registration Expiration Date: 2022-02-10T07:00:00Z<br>Registrar: NameSilo, LLC<br>Registrar IANA ID: 1479<br>Registrar Abuse Contact Email: abuse@namesilo.com<br>Registrar Abuse Contact Phone: +1.4805240066<br>Reseller: QHOSTER.COM<br>Domain Status: clientTransferProhibited<br>https://www.icann.org/epp#clientTransferProhibited<br>Registry Registrant ID:<br>Registrant Name: Robert Chris<br>Registrant Organization:<br>Registrant Street: 3126 Tea Berry Lane<br>Registrant City: Eau Claire<br>Registrant State/Province: WI<br>Registrant Postal Code: 54701<br>Registrant Country: US<br>Registrant Phone: +1.5185025850<br>Registrant Phone Ext:<br>Registrant Fax:<br>Registrant Fax Ext:<br>Registrant Email: zohoferdz1@gmail.com<br>Registry Admin ID:<br>Admin Name: Robert Chris<br>Admin Organization:<br>Admin Street: 3126 Tea Berry Lane<br>Admin City: Eau Claire<br>Admin State/Province: WI<br>Admin Postal Code: 54701<br>Admin Country: US<br>Admin Phone: +1.5185025850<br>Admin Phone Ext:<br>Admin Fax:<br>Admin Fax Ext:<br>Admin Email: zohoferdz1@gmail.com<br>Registry Tech ID:<br>Tech Name: Robert Chris<br>Tech Organization:<br>Tech Street: 3126 Tea Berry Lane<br>Tech City: Eau Claire<br>Tech State/Province: WI |

| | |
|---|---|
| | Tech Postal Code: 54701<br>Tech Country: US<br>Tech Phone: +1.5185025850<br>Tech Phone Ext:<br>Tech Fax:<br>Tech Fax Ext:<br>Tech Email: zohoferdz1@gmail.com<br>Name Server: NS65.DOMAINCONTROL.COM<br>Name Server: NS66.DOMAINCONTROL.COM<br>DNSSEC: unsigned |
| aerocerts.com | Domain Name: aerocerts.com<br>Registry Domain ID: 2590639617_DOMAIN_COM-VRSN<br>Registrar WHOIS Server: whois.namesilo.com<br>Registrar URL: https://www.namesilo.com/<br>Updated Date: 2021-02-11T07:00:00Z<br>Creation Date: 2021-02-10T07:00:00Z<br>Registrar Registration Expiration Date: 2022-02-10T07:00:00Z<br>Registrar: NameSilo, LLC<br>Registrar IANA ID: 1479<br>Registrar Abuse Contact Email: abuse@namesilo.com<br>Registrar Abuse Contact Phone: +1.4805240066<br>Reseller: QHOSTER.COM<br>Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited<br>Registry Registrant ID:<br>Registrant Name: Robert Chris<br>Registrant Organization:<br>Registrant Street: 3126 Tea Berry Lane<br>Registrant City: Eau Claire<br>Registrant State/Province: WI<br>Registrant Postal Code: 54701<br>Registrant Country: US<br>Registrant Phone: +1.5185025850<br>Registrant Phone Ext:<br>Registrant Fax:<br>Registrant Fax Ext:<br>Registrant Email: zohoferdz1@gmail.com<br>Registry Admin ID:<br>Admin Name: Robert Chris<br>Admin Organization:<br>Admin Street: 3126 Tea Berry Lane<br>Admin City: Eau Claire<br>Admin State/Province: WI<br>Admin Postal Code: 54701<br>Admin Country: US<br>Admin Phone: +1.5185025850<br>Admin Phone Ext:<br>Admin Fax:<br>Admin Fax Ext: |

| | |
|---|---|
| | Admin Email: zohoferdz1@gmail.com<br>Registry Tech ID:<br>Tech Name: Robert Chris<br>Tech Organization:<br>Tech Street: 3126 Tea Berry Lane<br>Tech City: Eau Claire<br>Tech State/Province: WI<br>Tech Postal Code: 54701<br>Tech Country: US<br>Tech Phone: +1.5185025850<br>Tech Phone Ext:<br>Tech Fax:<br>Tech Fax Ext:<br>Tech Email: zohoferdz1@gmail.com<br>Name Server: NS55.DOMAINCONTROL.COM<br>Name Server: NS56.DOMAINCONTROL.COM<br>DNSSEC: unsigned |
| napieslegal.com | Domain Name: napieslegal.com<br>Registry Domain ID: 2590704578_DOMAIN_COM-VRSN<br>Registrar WHOIS Server: whois.namesilo.com<br>Registrar URL: https://www.namesilo.com/<br>Updated Date: 2021-02-12T07:00:00Z<br>Creation Date: 2021-02-11T07:00:00Z<br>Registrar Registration Expiration Date: 2022-02-11T07:00:00Z<br>Registrar: NameSilo, LLC<br>Registrar IANA ID: 1479<br>Registrar Abuse Contact Email: abuse@namesilo.com<br>Registrar Abuse Contact Phone: +1.4805240066<br>Reseller: QHOSTER.COM<br>Domain Status: clientTransferProhibited<br>https://www.icann.org/epp#clientTransferProhibited<br>Registry Registrant ID:<br>Registrant Name: Robert Chris<br>Registrant Organization:<br>Registrant Street: 3126 Tea Berry Lane<br>Registrant City: Eau Claire<br>Registrant State/Province: WI<br>Registrant Postal Code: 54701<br>Registrant Country: US<br>Registrant Phone: +1.5185025850<br>Registrant Phone Ext:<br>Registrant Fax:<br>Registrant Fax Ext:<br>Registrant Email: zohoferdz1@gmail.com<br>Registry Admin ID:<br>Admin Name: Robert Chris<br>Admin Organization:<br>Admin Street: 3126 Tea Berry Lane<br>Admin City: Eau Claire |

| | |
|---|---|
| | Admin State/Province: WI<br>Admin Postal Code: 54701<br>Admin Country: US<br>Admin Phone: +1.5185025850<br>Admin Phone Ext:<br>Admin Fax:<br>Admin Fax Ext:<br>Admin Email: zohoferdz1@gmail.com<br>Registry Tech ID:<br>Tech Name: Robert Chris<br>Tech Organization:<br>Tech Street: 3126 Tea Berry Lane<br>Tech City: Eau Claire<br>Tech State/Province: WI<br>Tech Postal Code: 54701<br>Tech Country: US<br>Tech Phone: +1.5185025850<br>Tech Phone Ext:<br>Tech Fax:<br>Tech Fax Ext:<br>Tech Email: zohoferdz1@gmail.com<br>Name Server: NS19.DOMAINCONTROL.COM<br>Name Server: NS20.DOMAINCONTROL.COM<br>DNSSEC: unsigned |

| **.CA DOMAINS**<br>***Registrar***<br>**Key-Systems GmbH**<br>**Im Oberen Werk 1**<br>**66386 St. Ingbert**<br>**Germany** | |
|---|---|
| sllao.ca | Domain Name: sllao.ca<br>Registry Domain ID: 88831450-CIRA<br>Registrar WHOIS Server: whois.ca.fury.ca<br>Registrar URL: ksdomains.ca<br>Updated Date: 2021-02-22T10:47:09Z<br>Creation Date: 2021-02-05T17:58:44Z<br>Registry Expiry Date: 2022-02-05T17:58:44Z<br>Registrar: KS DOMAINS LTD<br>Registrar IANA ID: not applicable<br>Registrar Abuse Contact Email:<br>Registrar Abuse Contact Phone:<br>Domain Status: serverTransferProhibited<br>https://icann.org/epp#serverTransferProhibited<br>Registry Registrant ID: REDACTED FOR PRIVACY<br>Registrant Name: REDACTED FOR PRIVACY<br>Registrant Organization: REDACTED FOR PRIVACY<br>Registrant Street: REDACTED FOR PRIVACY |

| | |
|---|---|
| | Registrant City: REDACTED FOR PRIVACY<br>Registrant State/Province: REDACTED FOR PRIVACY<br>Registrant Postal Code: REDACTED FOR PRIVACY<br>Registrant Country: REDACTED FOR PRIVACY<br>Registrant Phone: REDACTED FOR PRIVACY<br>Registrant Phone Ext: REDACTED FOR PRIVACY<br>Registrant Fax: REDACTED FOR PRIVACY<br>Registrant Fax Ext: REDACTED FOR PRIVACY<br>Registrant Email: Please ask the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Other contacts of the queried domain name<br>Registry Admin ID: REDACTED FOR PRIVACY<br>Admin Name: REDACTED FOR PRIVACY<br>Admin Organization: REDACTED FOR PRIVACY<br>Admin Street: REDACTED FOR PRIVACY<br>Admin City: REDACTED FOR PRIVACY<br>Admin State/Province: REDACTED FOR PRIVACY<br>Admin Postal Code: REDACTED FOR PRIVACY<br>Admin Country: REDACTED FOR PRIVACY<br>Admin Phone: REDACTED FOR PRIVACY<br>Admin Phone Ext: REDACTED FOR PRIVACY<br>Admin Fax: REDACTED FOR PRIVACY<br>Admin Fax Ext: REDACTED FOR PRIVACY<br>Admin Email: Please ask the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Other contacts of the queried domain name<br>Registry Tech ID: REDACTED FOR PRIVACY<br>Tech Name: REDACTED FOR PRIVACY<br>Tech Organization: REDACTED FOR PRIVACY<br>Tech Street: REDACTED FOR PRIVACY<br>Tech City: REDACTED FOR PRIVACY<br>Tech State/Province: REDACTED FOR PRIVACY<br>Tech Postal Code: REDACTED FOR PRIVACY<br>Tech Country: REDACTED FOR PRIVACY<br>Tech Phone: REDACTED FOR PRIVACY<br>Tech Phone Ext: REDACTED FOR PRIVACY<br>Tech Fax: REDACTED FOR PRIVACY<br>Tech Fax Ext: REDACTED FOR PRIVACY<br>Tech Email: Please ask the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Other contacts of the queried domain name<br>Registry Billing ID: REDACTED FOR PRIVACY<br>Billing Name: REDACTED FOR PRIVACY<br>Billing Organization: REDACTED FOR PRIVACY<br>Billing Street: REDACTED FOR PRIVACY<br>Billing City: REDACTED FOR PRIVACY<br>Billing State/Province: REDACTED FOR PRIVACY<br>Billing Postal Code: REDACTED FOR PRIVACY |

| | |
|---|---|
| | Billing Country: REDACTED FOR PRIVACY<br>Billing Phone: REDACTED FOR PRIVACY<br>Billing Phone Ext: REDACTED FOR PRIVACY<br>Billing Fax: REDACTED FOR PRIVACY<br>Billing Fax Ext: REDACTED FOR PRIVACY<br>Billing Email: Please ask the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Other contacts of the queried domain name<br>Name Server: ina1.registrar.eu<br>Name Server: ina2.registrar.eu<br>Name Server: ina3.registrar.eu<br>DNSSEC: unsigned |

| **.CO DOMAINS**<br><br>***Registrar***<br>**NameSilo LLC**<br>**8825 N. 23rd Ave Suite 100**<br>**Phoenix, AZ 85021**<br>**United States** | |
|---|---|
| exarr.co | Domain Name: exarr.co<br>Registry Domain ID: DF12657D50CAF423A98C5A642371E41D2-NSR<br>Registrar WHOIS Server: whois.namesilo.com<br>Registrar URL: www.namesilo.com<br>Updated Date: 2021-02-14T17:54:46Z<br>Creation Date: 2021-02-09T17:54:42Z<br>Registry Expiry Date: 2022-02-09T17:54:42Z<br>Registrar: NameSilo, LLC<br>Registrar IANA ID: 1479<br>Registrar Abuse Contact Email: abuse@namesilo.com<br>Registrar Abuse Contact Phone: +1.4805240066<br>Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited<br>Registry Registrant ID: REDACTED FOR PRIVACY<br>Registrant Name: REDACTED FOR PRIVACY<br>Registrant Organization:<br>Registrant Street: REDACTED FOR PRIVACY<br>Registrant Street: REDACTED FOR PRIVACY<br>Registrant Street: REDACTED FOR PRIVACY<br>Registrant City: REDACTED FOR PRIVACY<br>Registrant State/Province: WI<br>Registrant Postal Code: REDACTED FOR PRIVACY<br>Registrant Country: US<br>Registrant Phone: REDACTED FOR PRIVACY<br>Registrant Phone Ext: REDACTED FOR PRIVACY<br>Registrant Fax: REDACTED FOR PRIVACY |

| | |
|---|---|
| | Registrant Fax Ext: REDACTED FOR PRIVACY<br>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.<br>Registry Admin ID: REDACTED FOR PRIVACY<br>Admin Name: REDACTED FOR PRIVACY<br>Admin Organization: REDACTED FOR PRIVACY<br>Admin Street: REDACTED FOR PRIVACY<br>Admin Street: REDACTED FOR PRIVACY<br>Admin Street: REDACTED FOR PRIVACY<br>Admin City: REDACTED FOR PRIVACY<br>Admin State/Province: REDACTED FOR PRIVACY<br>Admin Postal Code: REDACTED FOR PRIVACY<br>Admin Country: REDACTED FOR PRIVACY<br>Admin Phone: REDACTED FOR PRIVACY<br>Admin Phone Ext: REDACTED FOR PRIVACY<br>Admin Fax: REDACTED FOR PRIVACY<br>Admin Fax Ext: REDACTED FOR PRIVACY<br>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.<br>Registry Tech ID: REDACTED FOR PRIVACY<br>Tech Name: REDACTED FOR PRIVACY<br>Tech Organization: REDACTED FOR PRIVACY<br>Tech Street: REDACTED FOR PRIVACY<br>Tech Street: REDACTED FOR PRIVACY<br>Tech Street: REDACTED FOR PRIVACY<br>Tech City: REDACTED FOR PRIVACY<br>Tech State/Province: REDACTED FOR PRIVACY<br>Tech Postal Code: REDACTED FOR PRIVACY<br>Tech Country: REDACTED FOR PRIVACY<br>Tech Phone: REDACTED FOR PRIVACY<br>Tech Phone Ext: REDACTED FOR PRIVACY<br>Tech Fax: REDACTED FOR PRIVACY<br>Tech Fax Ext: REDACTED FOR PRIVACY<br>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.<br>Name Server: ns07.domaincontrol.com<br>Name Server: ns08.domaincontrol.com<br>DNSSEC: unsigned |