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.	Civil Action No: 1:19-cv-00716-ABJ

MICROSOFT'S BRIEF IN SUPPORT OF MOTION FOR DEFAULT JUDGMENT AND PERMANENT INJUNCTION

Plaintiff Microsoft Corporation ("Microsoft") seeks a default judgment and permanent injunction to prevent Defendants John Does 1-2 ("Defendants") from continuing to operate the malicious computer network infrastructure and Internet-based cybercriminal operation known as "Phosphorus." As set forth in Plaintiff's pleadings and the Court's previous orders, the Phosphorus infrastructure is comprised of Internet domains used to propagate and control the cybercrime operation, to infect end-user computers with malicious software ("malware") and to steal high-value, confidential and sensitive information from those end-user computers. Prior to issuance of this Court's Temporary Restraining Order, Preliminary Injunction, and Supplemental Preliminary Injunction, Defendants propagated and controlled the Phosphorus operation through Internet domains used to relay instructions to infected computers, including through abuse of Microsoft's Windows operating system. In particular, Defendants propagated and controlled the malicious infrastructure using domains that make deceptive use of Microsoft's trademarks and brands. Plaintiff now seeks to bring this case to final conclusion by way of a permanent

injunction that will prevent Defendants from continuing to propagate the Phosphorus operation or retaking control of that operation through abuse of Microsoft's trademarks and brands, once this case is closed.

Plaintiff requests an injunction (1) prohibiting Defendants from operating or propagating the Phosphorus infrastructure; (2) permanently transferring ownership to Microsoft of known malicious Phosphorus domains identified in the Court's prior injunction orders; and (3) adopting an expedited process for overseeing issues with Defendants' compliance with the permanent injunction including streamlined briefing and regular telephonic hearings to immediately resolve these issues either by appointing a Court Monitor or through another such process under this Court's supervision. This injunctive relief is required to prevent further harm to Plaintiff and the general public that would be caused if Defendants are able to continue to propagate and retake control of the Phosphorus infrastructure using Phosphorus domains that abuse Microsoft's trademarks and brands. A permanent injunction is the only way to afford relief and abate future harm in this case. This is particularly the case, given that, in the absence of such relief, the existing command and control domains would revert to Defendants and Defendants would certainly register new domains targeting Microsoft's trademarks and brands, use them to intrude upon Microsoft's Windows operating system and the computers of Microsoft's customers, grow and control the infrastructure, and steal high-value, confidential and sensitive information.

Defendants were properly served with Microsoft's complaint and other pleadings in this action and were provided with adequate notice of this action through means authorized by law, satisfying Due Process, satisfying Fed. R. Civ. P. 4 and reasonably calculated to provide Defendants with notice. Plaintiff served Defendants on March 27, 2019 and thereafter, by email and publication at the website http://www.noticeofpleadings.com/Phosphorus/, and more than 21

days have elapsed since Microsoft effected service. The Clerk was directed to enter default pursuant to Fed. R. Civ. P. 55(a) against John Does 1-2 for failing to appear after being properly provided notice of the proceedings under Fed. R. Civ. P. 4(f)(3) on October 8, 2019 and did so on October 9, 2019. *See* Dkt. No. 31. The factual allegations in the Complaint and the record in the case establish the elements of each of Plaintiff's claims and also establish the need for the requested injunctive relief.

II. FACTUAL BACKGROUND

This action arises out of violations of federal and state law caused by Defendants' operation of a harmful cybercriminal operation, known as "Phosphorus," carried out through harmful Internet domains. Defendants' illegal conduct includes the infection of computing devices running software licensed from Microsoft, the deep and persistent compromise of computing networks, the theft of sensitive information from those networks, and the use of Microsoft's famous trademarks, services, and products in the course of disguising and conducting illegal activity. 3/14/2019 Declaration of David Anselmi at ¶¶ 8-22, Dkt. No. 3-4.

Overview of Phosphorus

The group of Defendants known as "Phosphorus" specializes in targeting, penetrating, and stealing sensitive information from high-value computer networks connected to the Internet. Phosphorus continues to target political dissidents, activist leaders, religious organization, the Defense Industrial Base (DIB), journalists, and employees from multiple government agencies, including individuals protesting oppressive regimes in the Middle East. *Id.* ¶ 6.

Phosphorus intrude and cause injury to Microsoft and Microsoft's customers by damaging customer computers and software installed on their computers by sending deceptive email messages to victims with links to websites from which defendants install malicious

software onto the victims' computers, and then stolen information including credentials and sensitive user information may be transferred to defendants using command and control domains. *Id.* ¶ 20. Phosphorus has been active since 2013, and it poses a threat today and into the future. *Id.* ¶ 7. The specific identity of the Defendants is unknown. *Id.* ¶ 3. Information uncovered to date, and observations by others in the security community, indicate that it is likely that the Defendants are generally located in Iran.

After selecting a target organization, Defendants will typically attempt to compromise the computers of the targeted individual through a technique known as "spear phishing." *Id*. ¶ 8. In a typical spear phishing attack, Phosphorus sends the targeted individual an email specifically crafted so as to induce that individual to take some action that will lead to the compromise of their computer. *Id*. Phosphorus is able to craft the phishing email in a way that gives the email credibility to the target, often by making the email appear as if it was sent from an organization or person known to and trusted by the victim or concerning a topic of interest to the victim. *Id*. Phosphorus's emails often include links to websites that Phosphorus has set up in advance and controls. *Id.* ¶ 11. When the victim clicks on a link in the email, his or her computer is connected with the Phosphorus-controlled website. *Id*. The most vulnerable point in the Phosphorus defendants' operations are a number of Internet domains through which the Phosphorus defendants obtain victim credentials, log into compromised accounts, and review sensitive information from victim accounts. *Id*. ¶ 30.

The Court's Injunctions, Defendants' Disregard of the Injunctions, and Defendants' Continued Harmful Activities Through the Course of this Case

On March 15, 2019, the Court granted an Emergency Ex Parte Temporary Restraining Order ("TRO") tailored to halt the illegal activities and the growth of the Phosphorus operation. Dkt. No. 11. Through the Phosphorus operation, Defendants lure victims into clicking on links

embedded in personalized e-mails thereby compromising their computers, computer networks and accounts hosted on Microsoft's servers, all with the goal of stealing the victims' sensitive data. Defendants cause great harm to Microsoft by damaging the products that Microsoft licenses to its customers. Further, by exploiting Microsoft's famous and highly-regarded trademarks, products, and services to disguise and further its criminal conduct, Defendants cause Microsoft irreparable reputational and other harms for which no monetary recourse is available.

As explained in Microsoft's TRO Application, Defendants conduct their illegal operations by using an online command and control infrastructure consisting of a set of websites and domains. Dkt. No. 3-1 at 2. These domains are used both to break into computers and networks of the organizations that Phosphorus targets, control the reconnaissance of those networks, and, ultimately, exfiltrate sensitive information from them. To disable this command and control infrastructure, this Court ordered that these Phosphorus-controlled Internet domains, listed in the Appendix A be redirected to secure Microsoft servers. Dkt. No. 14. On April 12, 2019, the Court converted the TRO into a Preliminary Injunction. Dkt. No. 18. On May 22, 2019, Microsoft moved, and was granted, a supplemental preliminary injunction to capture a supplemental Appendix A with additional domains. Dkt. Nos. 19, 21. On July 18, 2019, Microsoft moved, and was granted, a second supplemental preliminary injunction to capture a second supplemental Appendix A with additional domains. Dkt. Nos. 24, 30. Defendants have added and continue to add new domains that cause harm to Microsoft and its customers in defiance of this Court's orders. 7/14/2019 Declaration of David Anselmi at ¶ 43, Dkt. Nos. 24-2.

Executing the Court's Temporary Restraining Order and Preliminary Injunction Orders, Microsoft cut communications between Defendants' existing command and control infrastructure and the victim computers and networks that Defendants attacked and from which

Defendants had been stealing information. 5/14/2019 Declaration of David Anselmi at ¶ 32, Dkt. No. 19-2. This effectively stymied Defendants' efforts to exploit the computers and networks they had targeted or already broken into.

However, Defendants, who are evidently resourceful and well-funded, continue to try to maintain and reestablish new command and control domains and other command and control infrastructure so that they can continue their illegal activities. Indeed, this probability was foreseen by the Court in issuing its TRO. And as foreseen, following the execution of the TRO, Preliminary Injunction, and Supplemental Preliminary Injunction, Defendants openly defied this Court and started to rebuild their command and control infrastructure by adding new Internet domains to Phosphorus' command and control infrastructure. *Id.* ¶¶ 9, 14. This Court then issued a Supplemental Preliminary Injunction Order allowing Microsoft to redirect 11 new Phosphorus-controlled domains to Microsoft secure servers. Dkt. No. 21. Defendants continued to ignore this Court's orders. This Court issued a Second Supplemental Preliminary Injunction Order allowing Microsoft to redirect 6 new Phosphorus-controlled domains to Microsoft secure servers. Dkt. No. 30; Dkt. No. 24-2 at ¶ 9. Yet, Defendants continue to defy this Court's orders, and there is a near-certain risk that they will attempt to do so going forward.

There is evidence that Defendants disregard for the Court's orders is knowing and intentional and that Defendants will continue to flout the Court's injunctions. First, Defendants have received service of process and repeated notice of the Court's injunctions. 9/13/2019 Declaration of Gabriel Ramsey in Support of Microsoft's Request for Entry of Default ("Ramsey Decl.") ¶¶ 16–18, Dkt. No. 28-1.

Second, after Defendants' infrastructure was disabled and Defendants were directed to cease their activities pursuant to multiple injunctions from this Court, the Defendants continued

to register and activate new domains for use in the same infrastructure and to target victims. Ramsey Decl. ¶ 6. This indicates that Defendants intentionally have, and are likely in the future to, violate any permanent injunction.

In the foregoing injunction orders, and consistent with the unrebutted allegations in the Complaint, the Court has made several factual findings and conclusions of law. Among other findings, the Court concluded that:

- The Court has jurisdiction;
- Defendants have used and have continued to use domains identified by Plaintiff throughout this case to control the Phosphorus infrastructure;
- Defendants have used and continue to use domains containing Microsoft's trademarks and brands to deceive victims and control the Phosphorus infrastructure;
- Defendants activities concerning the domains has violated or is likely to violate the Computer Fraud and Abuse Act (18 U.S.C. § 1020), 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 the common law doctrines of trespass to chattels, intentional interference with contractual relationships, unfair competition, unjust enrichment, and conversion;
- Unless enjoined, Defendants are likely to continue to engage in conduct that violates the Computer Fraud and Abuse Act (18 U.S.C. § 1020), 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 the common law doctrines of trespass to chattels, intentional interference with contractual relationships, unfair competition, unjust enrichment, and conversion;
- Defendants have received notice of the injunction and, despite that fact, have continued to and are likely to continue to register and use domains containing Microsoft's trademarks and brands to deceive victims and control the Phosphorus infrastructure;
- Defendants' conduct causes irreparable harm and such irreparable harm will continue unless the domains used by Defendants are disabled,

See Dkt. No. 11 at 2; Dkt. No. 18 at 2; Dkt. No. 21 at 2.

Discovery Efforts

In an attempt to obtain additional information regarding Defendants' identities, Plaintiff has served subpoenas on entities based in the United States in multiple rounds of discovery. Ramsey Decl. ¶ 26. Additionally, Plaintiff has made inquiries of entities outside of the United States. *Id.* Plaintiff pursued discovery of IP address, domain names, email address and credit cards in an attempt to more specifically identify Defendants. *Id.* ¶¶ 27–34.

However, given (a) Defendants' use of aliases and false information, (b) use of anonymous proxy computers or anonymization networks to create and maintain the infrastructure at issue in the case, (c) the absence of or limitations on the ability to carry out U.S.-style civil discovery outside of the U.S., (d) the ease with which anonymous activities can be carried out through the Internet, and (e) the sophistication of the Defendants in using tools to conceal more specific indicia of their identities or further contact information, Plaintiff was unable to specifically and definitively determine the "real" names and physical addresses of Defendants, to further attempts to enforce the injunctions against them and secure their compliance. *Id.*

Service of Process on Defendants

When the Court issued the TRO and Preliminary Injunction, the Court found good cause to permit service of Plaintiff's Complaint and related materials by alternative means pursuant to Rule 4(f)(3). Dkt. No. 11, ¶ 15 and pp. 9-10; Dkt. No. 18, ¶ 15 and p. 8. Beginning on March 27, 2019 and repeatedly thereafter, Plaintiff carried out service of process on Defendants by email to email addresses associated with Defendants' Internet domains and by publication on a public website www.noticeofpleadings.com/phosphorus/. Ramsey Decl. ¶¶ 18-20. The time for Defendants to answer or respond to the complaint expired 21 days after service, yet despite

repeated notice and service Defendants have not responded—despite evidence that they have opened Plaintiff's e-mails. Ramsey Decl. ¶ 23. The Clerk was directed to enter default pursuant to Fed. R. Civ. P. 55(a) against John Does 1-2 for failing to appear after being properly provided notice of the proceedings under Fed. R. Civ. P. 4(f)(3) on October 8, 2019 and did so on October 9, 2019. *See* Dkt. No. 31.

III. LEGAL STANDARD

Rule 55 of the Federal Rules of Civil Procedure provides that the clerk of the court must enter a party's default "[w]hen a party against whom a judgment for affirmative relief is sought has failed to plead or otherwise defend, and that failure is shown by affidavit or otherwise." Fed. R. Civ. P. 55(a). The Clerk's interlocutory "entry of default" pursuant to Federal Rule of Civil Procedure 55(a) provides notice to the defaulting party prior to the entry of default judgment by the court. In turn, Federal Rule of Civil Procedure 55(b)(2) authorizes courts to enter a default judgment when a defendant fails to defend a case or otherwise engages in dilatory tactics. *Teamsters Local 639-Employers Health Trust v. Boiler and Furnace Cleaners, Inc.*, 571 F. Supp. 2d 101, 106 (D.D.C. 2008). Default judgment is appropriate when the adversary process has been halted because of an unresponsive party. *Jackson v. Beech*, 636 F.2d 831, 836 (D.C. Cir. 1980) ("The default judgment must normally be viewed as available only when the adversary process has been halted because of an essentially unresponsive party."). Upon default, the well-pled allegations in a complaint as to liability are taken as true. *Ventura v. L.A. Howard Construction Co.*, 134 F. Supp. 3d 99, 103 (D.D.C. 2015) ("Default establishes the defaulting party's liability for the well-pleaded allegations of the complaint.") (internal quotations omitted). Here, the Clerk has entered Defendants' default under Rule 55(a), and Defendants received notice of same. Accordingly, given "the absence of any request to set aside the default or

suggestion by the defendant that it has a meritorious defense," default judgment is appropriate. *Serv. Emps. Int'l Nat'l Indus. Pension Fund v. Tandem Dev. Grp., LLC*, 274 F. Supp. 3d 1, 4 (D.D.C. 2017) (quoting *Int'l Painters & Allied Trades Indus. Pension Fund v. Auxier Drywall, LLC*, 531 F. Supp. 2d 56, 57 (D.D.C. 2008)).

In reviewing motions for default judgment, courts have referred to the following factors: (1) the amount of money involved in the litigation; (2) whether there are material issues of fact in the case needing resolution; (3) whether the case involves issues of great public importance; (4) whether the grounds for the motion for a default judgment are highly technical; (5) whether the party asking for a default judgment has been prejudiced by the non-moving party's actions or omissions; (6) whether the actions or omissions giving rise to the motion for a default judgment are the result of a good-faith mistake on the part of the non-moving party; (7) whether the actions or omissions giving rise to the motion for a default judgment are the result of excusable neglect on the part of the non-moving party; and (8) whether the grounds offered for the entry of a default judgment are clearly established. 10 C. Wright, A. Miller & M. Kane, Federal Practice and Procedure §§ 2684–85 (1990).

Courts may order permanent injunctive relief in conjunction with default judgments. *See, e.g.*, *Washington Metropolitan Area Transit Com'n v. Reliable Limousine Service, LLC*, 776 F.3d 1, 3 (D.C. Cir. 2015) (affirming default judgment that included a permanent injunction). Permanent injunctions depriving cybercrime defendants of their malicious infrastructure, on an ongoing basis in the future, have been entered by courts in connection with entry of default judgments. *See Microsoft Corp. v. John Does 1-8,* No. 1:14-CV-811, 2015 WL 4937441, at *1 (E.D. Va. Aug. 17, 2015) (O'Grady, J.) (adopting Report & Recommendation entering default judgment, issuing permanent injunction against John Does 1-8 and "their representatives and

persons who are in active concert or participation with them," and prohibiting them from sending malware code and content to specified internet domains); *Microsoft Corp. v. John Does 1-82,* No. 3:13-CV-00319-GCM, 2013 WL 6119242, at *4 (W.D.N.C. Nov. 21, 2013) (Mullen, J.) (same; restricting access and sending malicious software to Microsoft's licensed operating system and software and protected computers of Microsoft customers); *Consumer Source Holding, Inc. v. Does 1-24,* No. 1:13-CV-1512 AJT/JFA, 2014 WL 2967942, at *1 (E.D. Va. July 1, 2014) (same; restraining use of trademarks in connection with Internet websites); *Microsoft Corp. v. Does 1-2*, No. 1:16CV993, 2017 WL 5163363, at *3 (E.D. Va. Aug. 1, 2017), *report and recommendation adopted,* No. 116CV00993GBLTCB, 2017 WL 3605317 (E.D. Va. Aug. 22, 2017) (Lee, J.) (granting default judgment and permanent injunction and transferring control to Microsoft over domains and appointing Court Monitor to oversee defendants' compliance with permanent injunction); *see also* Order, *Microsoft v. John Does, 1-11*, No. 11CV00222 (W.D. Wash. Sept. 13, 2011), Dkt. No. 68 (Robart, J.) (granting default judgment and permanent injunction against Doe Defendants); *Microsoft Corp. v. Does*, No. 12-CV-1335 SJ RLM, 2012 WL 5497946, at *3 (E.D.N.Y. Nov. 13, 2012) (Johnson, J.) (granting motion for default judgment against Doe Defendants 1-21, 25-35, and 37-39).

IV. DISCUSSION

A. Due Process Has Been Satisfied

Plaintiff has served the complaint and other pleadings in this action on Defendants using the methods ordered by the Court under Rule 4(f)(3), including service by email and publication. It is well settled that legal notice and service by email, facsimile, mail and publication satisfies Due Process where these means are reasonably calculated, in light of the circumstances, to put defendants on notice. *See, e.g., Bazarian Int'l Financial Associates, L.L.C. v. Desarrollos*

Aerohotelco, C.A., 168 F. Supp. 3d 1, 13-14 (D.D.C. 2016) (acknowledging that courts have readily used Rule 4(f)(3) to authorize international service through non-traditional means); *Rio Props., Inc. v. Rio Int'l Interlink*, 284 F.3d 1007, 1014-15 (9th Cir. 2002) (involving Internet-based misconduct; "[Defendant] had neither an office nor a door; it had only a computer terminal. If any method of communication is reasonably calculated to provide [Defendant] with notice, surely it is email…");[1] Order at 4, *Microsoft Corp. v. John Does 1-27,* Case No. 1:10-cv-156 (E.D. Va. 2010), Dkt. No. 38 (Brinkema, J.) (authorizing service by email and publication in similar action). Email service and Internet publication are particularly appropriate here given the nature of Defendants' conduct and use of email as the primary means of communication in connection with establishing and managing the IP addresses and domains used to operate the Phosphorus domains and infrastructure. *Id*.

In this case, the email addresses provided by Defendants to the domain registrars, in the course of obtaining services that support Defendants' Phosphorus infrastructure, are the most accurate and viable contact information and means of notice and service. Indeed, the physical addressees provided by Defendants to domain registrars and other service providers are false and Defendants' whereabouts are unknown, and are not ascertainable despite the exercise of diligent formal and informal attempts to identify Defendants, which further supports service by email and publication. *Id*. Moreover, Defendants will expect notice regarding their use of the domain registrars' services to operate their Phosphorus infrastructure by email, as Defendants agreed to such in their agreements with the service providers who provided the domains for Defendants' use. *See Nat'l Equip. Rental, Ltd. v. Szukhent,* 375 U.S. 311 (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

[1] *Rio Properties* has been followed in the D.C. Circuit. *See U.S. ex rel. Barko v. Halliburton*, 952 F. Supp. 2d 108, 117 (D.D.C. 2013) (following *Rio*).

notice to be served by the opposing party, or even to waive notice altogether.").

Given the circumstances and Plaintiff's diligent efforts to locate Defendants, Due Process has been satisfied by Plaintiff's service by publication and multiple email notices.

B. Default Judgment is Appropriate

All of the relevant considerations point towards issuance of a default judgment against Defendants. First, the amount of money at stake weighs in favor of default judgment because Plaintiff is not requesting any monetary relief, and indeed it is not possible for Plaintiff to obtain any meaningful monetary relief under the circumstances. Accordingly, default judgment poses no risk of undue cost, prejudice, or surprise to Defendants.

Second, there are no material facts in dispute. Plaintiff has put forth a strong factual showing supported by forensic evidence and documentary evidence from researchers who have studied the Phosphorus infrastructure and its impact on victims. The allegations and evidence in the detailed Complaint and otherwise in the record establish that Defendants' conduct in operating the Phosphorus infrastructure violated and is likely in the future to violate the Computer Fraud and Abuse Act (18 U.S.C. § 1020), 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 the common law of trespass to chattels, intentional interference with contractual relationships, unfair competition, unjust enrichment, and conversion.

Third, this case involves a matter of substantial public importance. Defendants are perpetrating serious offenses and civil torts that cause substantial harm to hundreds if not thousands of victims. In addition to the general public interest in abating such harm, the public also has a strong interest in the integrity and enforcement of federal laws designed to deter

cybercrime and enhance data security.

Fourth, default here is not merely technical. This is not a situation where Defendants have accidentally missed a deadline by a few days; nor is default the result of a good faith mistake or excusable neglect. Rather, Defendants have affirmatively chosen not to appear and defend this action, despite ample notice and opportunity to do so. Plaintiff has made extraordinary efforts over the course of many months to ensure that Defendants were provided notice, and the evidence indicates that Defendants are actually aware of this action, but affirmatively choosing not to appear.

Fifth, Plaintiff and other victims of the Phosphorus infrastructure have been prejudiced by Defendants' actions and omissions. Defendants have refused to make their identities known and have refused to participate in this lawsuit. Defendants' disregard for this Court's process and refusal to communicate have caused Plaintiff to incur significant expense.

The grounds offered for the entry of a default judgment are clearly established.

C. Plaintiff Has Adequately Plead Each of its Claims

The Complaint alleges that Defendants have violated the Computer Fraud and Abuse Act ("CFAA") (18 U.S.C. § 1020), Electronic Communications Privacy Act (18 U.S.C. § 2701) ("ECPA"), the Lanham Act (15 U.S.C. §§ 1114, 1125), the Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)), and the common law doctrines of trespass to chattels, intentional interference with contractual relationships, unfair competition, unjust enrichment, and conversion. Each of these claims is adequately pled.

CFAA Claim. The CFAA penalizes a party that: (1) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage, 18 U.S.C. § 1030(a)(5)(C); or (2) intentionally accesses a computer without authorization or exceeds

authorized access, and thereby obtains information from any protected computer, 18 U.S.C. § 1030(a)(2)(C); or (3) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage to a protected computer, 18 U.S.C. § 1030(a)(5)(A). A "protected computer" is a computer "used in or affecting interstate or foreign commerce or communication." 18 U.S.C. 1030(e)(1); *see also Hedgeye Risk Management, LLC v. Heldman*, 271 F. Supp. 3d 181, 192 (D.D.C. 2017). 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 accesser is not entitled to obtain or alter." *Id.* at 193 (citing 18 U.S.C. § 1030(e)(6)). To prosecute a civil claim under the CFAA, a plaintiff must demonstrate loss or damage in excess of $5,000.

The Complaint alleges that Defendants have surreptitiously accessed protected computers by infecting the computers with malware and then using the Phosphorus infrastructure to control victim computers and to misappropriate confidential, sensitive and high-value information and in doing so have been damaged in an amount exceeding $5,000. Dkt. No. 1, ¶¶ 38-48. Plaintiffs have provided evidence that they have suffered in excess of $5,000 dollars, and the Court credited this evidence in granting preliminary injunctive relief. *See* Dkt. No. 11 at 2; Dkt. No. 18 at 2; Dkt. No. 21 at 2. Accordingly, Plaintiff has properly alleged a CFAA claim and is entitled to default judgment on this claim. Defendants' conduct is precisely the type of activity the CFAA is designed to prevent. *See e.g. Sandvig v. Sessions*, 315 F. Supp. 3d 1, 13 (D.D.C. 2018) (noting that a hacker cannot legally break into a Gmail account and copy the account-holder's emails and further stating that stealing another's credentials or breaching a site's security to evade a code-based restriction is unprotected by the First Amendment); *Roe v. Bernabei & Wachtel PLLC*, 85 F. Supp. 3d 89, 102 (D.D.C. 2015) (quoting *Lewis-Burke Assocs., LLC v. Widder*, 725 F. Supp.

2d 187, 194 (D.D.C. 2010) ("The Computer Fraud and Abuse Act, 18 U.S.C. §1030, is intended "primarily to deter computer hacking.")); *Facebook, Inc. v. Fisher*, 2009 U.S. Dist. LEXIS 122578 (N.D. Cal. 2009) (CFAA violation where defendants allegedly engaged in a phishing and spamming scheme that compromised the accounts of Facebook users); *Physicians Interactive v. Lathian Sys., Inc.*, 2003 U.S. Dist. LEXIS 22868, *25 (E.D. Va. 2003) (CFAA violation where the defendant hacked into a computer and stole confidential information); *Microsoft Corp. v. Doe*, 2015 U.S. Dist. LEXIS 109729 (E.D. Va. Aug. 17, 2015) (O'Grady, J.) (CFAA violation for operating botnet); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 46951 (E.D. Va. Apr. 2, 2014) (Brinkema, J.) (same).

ECPA Claim. The 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). Persons injured by violations of the ECPA may bring a civil suit to obtain injunctive relief and damages. *E.g.*, *Council on American-Islamic Relations Action Network, Inc. v. Gaubatz*, 31 F. Supp. 3d 237 (D.D.C. 2014).

The Complaint alleges that Plaintiff's servers and its licensed operating system at end user computers are facilities through which electronic communication services are provided. Dkt. No. 1, ¶¶ 21-37, 49-54. Defendants' conduct in operating Phosphorus violates the ECPA because Defendants break into computing devices and computer networks with the direct intention of acquiring the contents of sensitive communications whether e-mails, voice mails, or other communications types. *Id.* Defendants use software, installed without authorization on compromised computers to do so. *Id.* Obtaining stored electronic information in this way,

without authorization, is a violation of the Electronic Communications Privacy Act. *See Council on American-Islamic Relations Action Network, Inc. v. Gaubatz*, 667 F. Supp. 2d 67, 71-73 (D.D.C. 2009); *Microsoft Corp. v. Does 1-18,* No. 1:13CV139 LMB/TCB, 2014 WL 1338677, at *7 (E.D. Va. Apr. 2, 2014) (finding violation of ECPA where "Defendant's Bamital botnet used computer codes to hijack internet browsers and search engines by intercepting communications to and from Microsoft servers, and forcing end-users to visit certain websites" which was done "without the end-users' consent, and allowed defendant to monetize end-users' forced activities"). Accordingly, Plaintiff properly alleged an ECPA claim and default judgment on this claim is warranted.

Lanham Act Claims. Section 1114(1) 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. *See* § 15 U.S.C. § 1114; *see also Two Pesos, Inc. v. Taco Cabana, Inc.*, 505 U.S. 763, 763 (1992); *Yah Kai World Wide Enterprises, Inc. v. Napper*, 195 F. Supp. 3d 287, 309 (D.D.C. 2016). Here, the Complaint alleges that Defendants use Microsoft's registered, famous and distinctive trademarks in Internet domains designed to deceive victims into clicking on the links in emails and to blend in with normal network traffic, when those domains are being used to unlawfully send commands to victim computers or exfiltrate sensitive stolen data. In this way, Defendants deceive victims, cause them confusion and cause them to mistakenly associate Microsoft with this activity. Dkt. No. 1, ¶¶ 22-37. Defendants' conduct also constitutes false designation of origin under section 1125(a), causing confusion and mistakes as to Plaintiff's affiliation with Defendants' malicious conduct. *See, e.g., Am. Ass'n for Advancement of Sci. v. Hearst Corp.*, 498 F. Supp. 244, 259-61 (D.D.C. 1980). The Complaint alleges this Lanham Act

violation in detail as well. Dkt. No. 1, ¶¶ 21-37, 55-60. Microsoft has also stated a dilution claim as (1) its marks are "distinctive and famous," (2) defendants abused the marks when they were already famous, and (3) defendants mark dilutes the famous mark. *Appleseed Foundation, Inc. v. Appleseed Inst., Inc.*, 981 F. Supp. 672, 677 (D.D.C. 1997); Dkt. No. 1, ¶¶ 61-66. Thus, Plaintiff properly alleged these Lanham Act claims and default judgment is warranted.

ACPA Claim. To succeed on an ACPA claim, Plaintiff must demonstrate that: (1) its trademark is a distinctive or famous mark entitled to protection; (2) Defendants' domain name is identical or confusingly similar to Plaintiff's mark; and (3) Defendants "register[], traffic[] in, or use[]" a domain name with the bad faith intent to profit from it. *Xereas v. Heiss,* 933 F. Supp. 2d 1, 14-17 (D.D.C. 2013) (quoting 15 U.S.C. § 1125(d)(1)(A)); *Hanley-Wood LLC v. Hanley Wood LLC*, 783 F. Supp. 2d 147, 152 (D.D.C. 2011). Here, the Complaint alleges that Defendants use Microsoft's registered, famous, and distinctive trademarks in many domains they have registered. Dkt. No. 1, ¶¶ 21, 25-26, 36, 38, 40, 72-77. For example, Microsoft's registered, famous, and distinctive trademarks include "Microsoft," "Windows," "Outlook," "Hotmail," and "OneDrive," among others. Dkt. No. 1, Appendix B. The Complaint establishes that Defendants have acted in bad faith with the intent to profit from Microsoft's trademarks. Defendants have no trademark or IP rights in the domain names; the domain names do not consist of a name used to identify Defendants; Defendants have not used the domain name in connection with the bona fide offering of any goods or services; Defendants use of the domains to exfiltrate sensitive information from a victim's network harms the goodwill represented by Microsoft's trademarks; Defendants used false information to register the domains; and Defendants registered multiple domains that incorporate Microsoft's distinctive marks. *See id.* These factors demonstrate an ACPA violation. *See Hanley-Wood*, 783 F. Supp. 2d at 152-53.

Accordingly, Plaintiff properly alleged an ACPA claim and default judgment on this claim is warranted.

Tort Claims. Under District of Columbia law, the tort of conversion 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) (denying summary judgment on conversion claim relating to disputed ownership of laptop computer which allegedly contained personal files and software). The related tort of trespass to chattels applies where a defendant "intentionally dispossess[es] another of the chattel, or (b) us[es] or intermeddle[es] with a chattel in the possession of another." *E. Savings Bank, FSB v. Papageorge*, 31 F. Supp. 3d 1, 20 (D.D.C. 2014) (quoting *Hornbeck Offshore Transp., LLC v. United States*, 563 F. Supp. 2d 205, 212 n.8 (D.D.C. 2008)). Here, the Complaint establishes that Defendants exercised dominion and authority over Plaintiff's proprietary Windows software by injecting code that fundamentally changed important functions of the software, converted Plaintiff's property, and were unjustly enriched with ill-gotten benefits reaped from the Phosphorus infrastructure and its victims. Dkt. No. 1 at ¶¶ 21-42, 78-91; *see also Microsoft Corp.*, 2014 WL 1338677, at **9-10 (finding plaintiff alleged sufficient facts on conversion and trespass to chattel claims to where defendant via its Bamital botnet 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).

Defendants' conduct resulted in unjust enrichment as well because "[w]ithout authorization, defendant used Microsoft's servers, networks, Windows operating system, Internet Explorer, and Bing search engine to operate and propagate the Bamital botnet click-fraud

scheme" and profited from this activity such that it "would be inequitable for defendant to retain the benefits from this unlawful scheme." *Id.* at *10.

Defendants' conduct also constitutes a clear case of intentional interference with Microsoft's contractual relationships with customers of its Windows products. *See, e.g., Banneker Ventures, LLC v. Graham*, 225 F. Supp. 3d 1, 14 (D.D.C. 2016) (denying motion to dismiss tortious interference claims since there was a valid contract of which the interferer had knowledge and intentional interference caused termination of contract or failure of performance resulting in damages); *Park v. Hyatt Corp.*, 436 F. Supp. 2d 60, 64-65 (D.D.C. 2006) (holding that a defendant can be liable for interference by affecting not only a third-party's ability to maintain a contract, but also a plaintiff's ability to maintain a contract).

Defendants' conduct also amounts to unfair competition since it is based on acts including "false advertising or deceptive packaging likely to mislead customers into believing goods are those of a competitor." *Hanley Wood LLC,* 783 F. Supp. 2d at 153.

The well-pled allegations in Plaintiff's Complaint, which set forth the elements of each of Plaintiffs' claims, are taken as true given Defendants' default. *Ventura v. L.A. Howard Construction Co.*, 134 F. Supp. 3d 99, 103 (D.D.C. 2015) ("Default establishes the defaulting party's liability for the well-pleaded allegations of the complaint.") (internal quotations omitted). Accordingly, the only question is what remedy to afford Plaintiff.

D. A Permanent Injunction Should Issue to Prevent Further Irreparable Harm

A permanent injunction is appropriate where: (1) plaintiff has suffered an irreparable injury; (2) remedies available at law (e.g. monetary damages), are inadequate to compensate for that injury; (3) considering the balance of hardships between plaintiff and defendant, a remedy in equity is warranted; and (4) the public interest would not be disserved by a permanent injunction.

Monsanto Co. v. Geerton Seed Farms, 561 U.S. 139, 156-57 (2010) (quoting *eBay Inc. v. MercExchange, L.L.C.*, 547 U.S. 388, 391 (2006)); *see also District Title v. Warren*, 2015 WL 7180200, at *10 (D.D.C. Nov. 13, 2015).

1. Plaintiff Has Suffered and Is Likely to Suffer Irreparable Injury That Cannot Be Compensated Monetarily.

Consumer confusion and injury to business goodwill constitute irreparable harm. *See, e.g., United States Dep't of Justice v. Daniel Chapter One*, 89 F. Supp. 3d 132, 145 (D.D.C. 2015) (granting a permanent injunction "in order to protect the public" from deceptive advertising claims); *Hanley-Wood LLC v. Hanley Wood LLC*, 783 F. Supp. 2d at 147 (granting entry of permanent injunction to prevent misappropriation of Plaintiff's business goodwill and future false advertising); *Partido Revolucionario Dominicano (PRD) Seccional Metropolitana de Washington-DC, Maryland y Virginia v. Partido Revolucionario Dominicano, Seccional de Maryland y Virginia*, 312 F. Supp. 2d 1, 16 (D.D.C. 2004) (entering permanent injunction in light of plaintiff's loss of control over its reputation and injury to its goodwill); *Malarkey-Taylor Assocs., Inc. v. Cellular Telecomms. Indus.*, 929 F. Supp. 473, 478 (D.D.C. 1996) (citations omitted); *AARP v. Sycle,* 991 F. Supp. 2d 224, 230 (D.D.C. 2013) (granting permanent injunction where "Defendant has continued to use the [plaintiff's] Marks to sell insurance services, despite issuance of a demand letter and filing of the instant lawsuit" based on the presumption of harm in trademark infringement cases). The Court previously found that the harm caused to Plaintiff by the Phosphorus operations, in particular the confusing and misleading use of Microsoft trademarks and brands, constitutes irreparable harm. Dkt. No. 21 at 2. To the extent that Defendants are able to continue to use domains bearing Microsoft's trademarks and brands in furtherance of their activities, such irreparable harm would certainly continue in the future.

This finding is consistent with several cases that have concluded that computer malware

operations and associated use of Microsoft's trademarks cause irreparable harm. *See, e.g., Microsoft Corp. v. Peng Yong et al.*, Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.) (injunction to dismantle botnet command and control servers); *Microsoft v. Piatti, et al.*, Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.) (injunction to dismantle botnet command and control servers); *Microsoft Corporation v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va., Brinkema J.) (same); *Microsoft v. John Does 1-11*, Case No. 2:11-cv-00222 (W.D. Wa. 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.) (injunction disconnecting service to botnet hosting company).

In addition to the irreparable harm caused to Plaintiff's goodwill, even the monetary harm caused by Defendants is and will be irremediable absent an injunction because Defendants are elusive cybercriminals whom Plaintiff is unlikely to be able to enforce a judgment against. *See, e.g., 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 Rept., 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); *Advanta Bank v. F.D.I.C.,* 684 F. Supp. 2d 17, 28 (D.D.C. 2010) (finding "likelihood that it will become at best another creditor in bankruptcy of an insolvent bank establishes a sufficient showing of irreparable harm").

2. The Balance of Equities Strongly Favors an Injunction.

Because Defendants are engaged in an illegal scheme to defraud computer users and injure Plaintiff, the balance of equities clearly tips in favor granting a permanent injunction. *See, e.g., Grace v. Whitaker*, 344 F. Supp. 3d 96, 146 (D.D.C. 2018) (quotations omitted); *DL v. District of Columbia*, 194 F. Supp. 3d 30, 98 (D.D.C. 2016) ("An injunction requiring

[Defendant] to do nothing more than comply with its legal obligation cannot, by definition, harm it.")). On one side of the scales of equity rests the harm to Plaintiff and its customers caused by Defendants' ongoing Phosphorus operation, including ongoing deceptive use of Plaintiff's trademarks and brands in the Phosphorus domains. By contrast, on the other side, rests no legally cognizable harm to Defendants because an injunction would only require them to cease illegal activities. For this reason, an ongoing permanent injunction is appropriate. *See id*.

3. An Injunction is in the Public Interest.

The public interest is clearly served by enforcing statutes designed to protect the public, such as the Lanham Act, CFAA, and ECPA. *See, e.g.*, *Sycle*, 991 F. Supp. 2d at 224 (finding that "the public interest favors protecting against further violation of federal trademark law"); *Lifted Research Grp. v. Behdad, Inc.*, 591 F. Supp. 2d 3, 8 (D.D.C. 2008) ("The Court further finds that an injunction would not harm others, and that public interest favors protecting against further violation of federal copyright and trademark law."); *Breaking the Chain Found., Inc. v. Capital Educ. Support, Inc.*, 589 F. Supp. 2d 25, 30 (D.D.C. 2008) (same); *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").

Here, Plaintiff requests an injunction that will transfer permanent control of the existing Phosphorus domains to Microsoft and adoption of an expedited process for overseeing issues with Defendants' compliance with the permanent injunction including streamlined briefing and regular telephonic hearings to immediately resolve these issues either by appointing a Court Monitor pursuant to Federal Rule of Civil Procedure 53, or through another such process under this Court's supervision. Given Defendants' conduct to date including ignoring this Court's existing injunctive orders and continuing to add new domains, Microsoft believes this Court

needs to establish a mechanism to quickly disable and transfer new malicious domains that are put into operation by Defendants that deceive computer users, issue instructions to infected computers, take control over them, and exfiltrate high-value, sensitive and confidential information and protect Microsoft and its customers.

Given the risks the public will face absent an injunction, the calculus is clear. There is no risk that the injunction will impact any legitimate interest of any party. Neither Defendants nor any other party has come forward to assert any undue impact by Microsoft's control of the existing Phosphorus domains. In particular, the third-party domain registries responsible for administering the Phosphorus Defendants' domains must simply carry out routine actions that they would take in the ordinary course of their business, namely transferring the domains to the permanent control of Plaintiff.

Directing such routine actions and reasonable cooperation to vindicate the public's interest, and ensure that the permanent injunction is not rendered fruitless, is authorized by the All Writs Act (28 U.S.C. § 1651(a) and the Court's equitable authority), will not offend Due Process, does not interfere with normal operations, does not deprive any third party of any property interest and requires Microsoft to compensate the third parties for the assistance rendered.[2] Indeed, Plaintiff has conferred with relevant domain registries, and they have no

[2] The All Writs Act provides that a court may issue all writs necessary or appropriate for the administration of justice. 28 U.S.C. § 1651(a); *see United States v. New York Tel. Co*., 434 U.S. 159, 174 (1977) (authorizing order to third-party telephone company to assist in implementation of a pen register warrant); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398, 30 (E.D. Va. Jan. 6, 2014) (authorizing relief similar to that requested herein); *Sarnecka-Crouch v. Billington,* No. 06-1169 ESH, 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 plaintiff's Social Security benefits account for the period 2005-2009); *Evans v. Williams,* No. 76-293, 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

objection to the requested relief.

4. An Ongoing Process is Needed to Efficiently and Effectively Curtail Defendants' Efforts to Rebuild Phosphorus' Command and Control Infrastructure.

Defendants are persistent in their activities and are likely to attempt to maintain, rebuild, and even grow, their capabilities again and again. Plaintiff will, as it has up until now, monitor Defendants' activities, identify new Phosphorus command and control domains associated with Microsoft's trademarks or brands ("Phosphorus Domains") as they are activated. Indeed, as discussed above, Defendants have continued to put into operation new Phosphorus Domains throughout the course of this case, and the only process that will allow those domains to be immediately disabled, stopping the harm, is this Court or the Court Monitor's continued oversight of the existing injunctions.

Defendants have even demonstrated willful violation of the Court's prior orders by registering new harmful domains using Microsoft's own contact information, to deceive victims. Consequently, Plaintiff and the Court face the nearly certain prospect that enforcing the Court's permanent injunction will require continuously re-opening the case and multiple ongoing rounds of motion practice and amendments to the list of command and control domains subject to the Court's permanent injunction and multiple new proceedings. Failing this sustained effort, Defendants will and have continued their malicious and illegal activities, causing irreparable injury to Plaintiff, its customers and the public in defiance of this Court's orders. *See e.g.* Dkt. No. 19-2 at ¶ 32; Dkt. No. 24-2 at ¶¶ 9, 43.

A critical requirement for effective relief is that command and control domains be

power under the All Writs Act) (citing *New York Tel. Co*., 434 U.S. at 172); *Dell, Inc. v. Belgiumdomains, LLC*, 07-22674, 2007 WL 6862341, at *6 (S.D. Fla. Nov. 21, 2007) (All Writs Act applied in conjunction with trademark seizure under Rule 65 and Lanham Act).

transferred as quickly as they are identified. Defendants are able to put into place such malicious infrastructure and to operationalize it, in an extremely rapid and dynamic manner. Dkt. No. 24-2 at ¶¶ 30-34, 43. Accordingly, for the Court's relief to be effective, to mitigate injury and to prevent ongoing violations, and to meet this dynamic threat, it is necessary that any permanent injunction include enforcement mechanisms that achieve the same speed and scale that can be achieved by Defendants. *Id.* ¶ 43. Without a mechanism that achieves the goal of speed, these sophisticated Defendants will be able to take advantage of how quickly infrastructure can be assembled on the Internet, and would be able to evade the Court's injunction.

Plaintiff therefore requests that this Court adopt an expedited process for overseeing issues with Defendants' compliance with the permanent injunction including streamlined briefing and regular telephonic hearings to immediately resolve these issues. Plaintiff acknowledges the burden that such a sustained effort would place on the Court, which is why it requests that this process be overseen by a Court Monitor, as set forth below and as set forth in the proposed permanent injunction. However, even if this Court is not inclined to appoint a Court Monitor, Plaintiff would request that this Court administer a similarly streamlined, expedited process that results in prompt relief and an effective injunction. Plaintiff is, of course, open to alternative procedures that achieve the same goals, if the Court prefers to directly administer such processes. However, as set forth below, there is precedent for appointment of a Court Monitor in a very similar situation. Such a procedure readily affords the speed necessary for effective relief, provides for Court oversight and continuous reporting, and has proven to be effective in enforcement of permanent injunctions in matters involving cybercrime infrastructure.

Plaintiff has sought and been granted implementation of a streamlined process overseen by a Court Monitor in a similar case. *See, e.g.*, *Microsoft Corp. v. John Does 1-2*, Civil Action

No. 1:16-cv-993 (E.D. Va. Dec. 6, 2016) (Lee, J.) (appointing a court monitor to oversee enforcement and administration of permanent injunction relating to cybercrime "Strontium domains"). Plaintiff believes the availability of a Court Monitor to oversee this process will increase the effectiveness of any permanent injunction order, as it will enable more prompt, continuous response to Defendants' continued violation of any permanent injunction. The Court Monitor will make determinations on any disputes between Plaintiff, any Defendant, registry or other third party, regarding disabling of Phosphorus Domains as set forth in the Proposed Order Granting Microsoft's Motion for Default Judgment and Permanent Injunction submitted with this Motion. The Court Monitor will further determine (based on evidence submitted by Microsoft) whether Defendant is violating the permanent injunction, will determine whether additional particular domains are in fact being used by Defendants as part of Phosphorus, and may order that such new domains be added to the list of domains subject to the Court's permanent injunction.

Under Federal Rule of Civil Procedure 53(a)(1)(C), a court may appoint a court monitor to "address pretrial and posttrial matters that cannot be effectively and timely addressed by an available district judge or magistrate judge of the district." A court monitor would be effective here because it will impose an undue burden on the court's limited time and resources to rule on what are expected to be continuous and potentially frequent motions to amend the permanent injunction every time Defendants register and use new Phosphorus Domains leveraging Microsoft trademarks or targeting Microsoft's software or services. This is especially the case considering the ease and speed with which Defendants are currently registering Microsoft-related domains to continue their attacks, throughout the course of this case. Further, the ability of a court monitor to make determinations on such matters will increase the effectiveness of the

Court's permanent injunction and permit enforcement of Defendants' compliance on an ongoing basis.

Courts have frequently made use of court-appointed monitors and other masters in cases such as this one, where ongoing compliance with the court's permanent injunction is at issue and supervision has the prospect of being time-consuming or difficult for the court to undertake without assistance. *See e.g.*, *Ohio Valley Envtl. Coal. v. Fola Coal Co., LLC*, No. 2:13-21588, 2016 U.S. Dist. LEXIS 73904, at *50 (S.D. W. Va. June 7, 2016) ("Appointing a special master is proper in this case because the proposed injunctive relief includes complex analysis and implementation of environmental engineering plans and monitoring to correct [defendant's] violations."); *Microsoft Corp. v. John Does 1-2*, Civil Action No. 1:16-cv-993 (E.D. Va. Dec. 6, 2016) (Lee, J.) (appointing a court monitor to oversee enforcement and administration of permanent injunction relating to cybercrime "Strontium domains"); *Schaefer Fan Co. v. J & D Mfg., Inc.*, 265 F.3d 1282 (Fed. Cir. 2001) (appointing special master to resolve disputes and issue decisions regarding compliance with settlement agreement); *Evans v. Fenty*, 701 F. Supp. 2d 126, 129 (D.D.C. 2010) (Special Masters assisted court by making findings and recommendations that addressed the status of defendants' compliance and available options for curing the identified deficiencies); *see also* 18 U.S.C. § 1836(b)(2)(D) (providing that special masters may be appointed to locate and isolate trade secret information from other property).

In the streamlined process in the proposed permanent injunction, Plaintiff will monitor Defendants' activities and will identify new Microsoft-related Phosphorus Domains as Defendants activate them. Making an accurate identification is crucial, and Plaintiff will base its conclusions on a set of criteria developed over the course of its lengthy investigation into Defendants and Phosphorus. Dkt. No. 24-7 at 8-10, Dkt. No. 24-2, ¶¶ 35-42 and Ex. 2.

"Phosphorus Domains" are domains which are determined to meet the following two criteria:

Criteria 1: The domains are used by Defendants to break into computers and networks of the organizations that Phosphorus targets, or control the reconnaissance of those networks, or, ultimately, exfiltrate sensitive information from them, or are otherwise used by Defendants to carry out the activities and purposes prohibited by this Permanent Injunction. A domain is determined to be a Phosphorus Domain by comparing the activities and patterns associated with that domain with known confirmed Phosphorus Domains. The following factors concerning the domain will be used in this analysis:

Delivers malicious software, code, commands, exploits and/or "backdoor" functionality previously associated with Phosphorus, including but not limited to: Stealer malware, or similar code or functionality deployed in a manner previously associated with Phosphorus.	Associated with remote code execution through browser drive-by or malicious attachment, privilege escalation or sandbox escape, security feature bypass, social engineering based attack and/or bootstrapped add-on, escalation of privileges, DLL file backdoor, credential stealing functionality, SSL tunnel, and/or functionality to deliver code or functions to "air gapped" USB devices, deployed in a manner previously associated with Phosphorus or similar code or functionality.
Domain registration information	Use of cryptocurrency to purchase services
Name servers	Start of Authority (SOA) records
Resolves to IP of past Phosphorus domain, command and control server or similar infrastructure	Resolves to IP used in past Phosphorus malware delivery or credential harvesting domains or credential harvesting domains
Used to deceive, target, obtain information from, and/or communicate commands or code to recipients, persons, institutions or networks previously targeted by Phosphorus.	Used to deceive, target, obtain information from, and/or communicate commands or code to recipients that may possess or be able to provide sensitive information or trade secrets of persons, entities or networks related to the defense, critical infrastructure or high technology sectors, journalists, political advisors or organizations, government bodies, diplomatic institutions, religious organizations, universities, and/or military forces and installations.
SSL Cert Issuer_DN	SSL Cert Subject_DN
Host	Registrar
Domains similar to previously used domains	Victims being targeted similar to past targets

Dkt. No. 24-2, ¶¶ 35-42 and Ex. 2.

Criteria 2: The domains (a) use and infringe Microsoft's trademarks, trade names or service marks or confusingly similar variants, or (b) use any false or deceptive designation, representation or description, which would damage or injure Microsoft or give Defendants an unfair competitive advantage or result in deception of consumers, or (c) suggest in any way that Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Microsoft, or pass off Defendants' activities, products or services as Microsoft's. Such trademarks and brands shall include, but are not limited to the following trademarks, brands and/or confusingly similar variants: While Defendants may use any Microsoft marks, brands or confusingly similar indicators, Defendants have already exploited or are likely to exploit the following: "365," "Azure," "Bing," "Excel," "Exchange," "Healthvault," "Hotmail," "LinkedIn," "Live," "Messenger," "Microsoft," "Minecraft," "MSDN," "MSFT," "MS," "MSN," ".NET," O365," "Office," "OneDrive," "Outlook," "OWA," "Passport," "PowerPoint," "SharePoint," "Skype," "Surface," "Visio," "Win," "Windows," and "Xbox." Also, Criteria 2 is met where defendants use generalized versions of terms that are suggestive of Microsoft's services, but do not specifically use a trademark. Dkt. No. 24-2, ¶¶ 35-42 and Ex. 2.

With respect to domains alleged to meet the criteria to constitute Phosphorus Domains, and domains that are alleged to be Phosphorus Domains based on new criteria not listed in this Order, Microsoft shall submit a written motion to this Court or the Court Monitor seeking a declaration that such domains are Phosphorus Domains. This Court or the Court Monitor shall take and hear evidence and shall make determinations and issue orders whether domains are Phosphorus Domains, as set forth in the proposed permanent injunction submitted with this motion.

Plaintiff believes that this process will reduce the burden on the Court, better ensure

enforcement of the Court's permanent injunction, provide for efficient reaction against Defendants as they attempt to activate new domains for illegal ends, and provide an adequate mechanism for registries, third-parties, or Defendants to challenge the substance and process concerning enforcement of the permanent injunction. Thus, the appointment of a court monitor in this case is appropriate under Federal Rule of Civil Procedure 53(a)(1)(C).

If the Court elects to appoint a Court Monitor to oversee ongoing enforcement of the permanent injunction as set forth in the Proposed Order Granting Microsoft's Motion for Default Judgment and Permanent Injunction, Plaintiff respectfully requests that the Court appoint the Honorable Faith Hochberg (Ret.) who has experience with the above-outlined process, the technical and legal issues in this case, has relevant legal and technical expertise based on other matters and has served in the capacity as a neutral special master in prior matters. Any Court Monitor must establish that there are no conflicts of interest and provide an affidavit "disclosing whether there is any ground for disqualification under 28 U.S.C. § 455." This Court has already received an affidavit at Dkt. No. 24-9 establishing suitability for the role of Court Monitor, including current curriculum vitae, and the record shows no grounds for disqualification.

V. CONCLUSION

For the reasons set forth in this brief, and based on the Complaint, the evidence submitted in this case and the Court's prior orders, Plaintiff respectfully requests that the Court grant Microsoft's Motion for Default Judgment and Permanent Injunction.

Dated: October 21, 2019

Respectfully submitted,

/s/ *Gabriel M. Ramsey*

Gabriel M. Ramsey (*pro hac vice*)
CROWELL & MORING LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111
Telephone: (415) 986-2800
Fax: (415) 986-2827
gramsey@crowell.com

Julia R. Milewski (D.C. Bar No. 1008678)
Justin D. Kingsolver (D.C. Bar. No. 1033806)
Matthew B. Welling (*pro hac vice*)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Telephone: (202) 624-2500
Fax: (202) 628-5116
jmilewski@crowell.com
jkingsolver@crowell.com
mwelling@crowell.com

Richard Domingues Boscovich (*pro hac vice*)
MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052-6399
Telephone: (425) 704-0867
Fax: (425) 936-7329
rbosco@microsoft.com

Attorneys for Plaintiff Microsoft Corp.