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

DXC TECHNOLOGY COMPANY, a Nevada corporation, Plaintiff, v. JOHN DOES 1-2, Defendants.	Civil Action No: 1:20-cv-00814

MEMORANDUM IN SUPPORT OF DXC'S MOTION FOR DEFAULT JUDGMENT AND PERMANENT INJUNCTION

I. INTRODUCTION

Plaintiff DXC Technology Company ("DXC") seeks a default judgment and permanent injunction to prevent Defendants John Does 1-2 from continuing to operate the malicious software used to engage in a coordinated cyberattack against DXC. As set forth in Plaintiff's pleadings and the Court's previous orders, Defendants used Internet domains known as Command and Control Infrastructure to attack DXC's systems or infrastructure in order to exfiltrate information from those systems. Through this request, Plaintiff seeks to bring this case to final conclusion by way of a permanent injunction that will prevent Defendants from continuing to propagate its attack or retaking control of its operation once this case is closed.

Plaintiff requests an injunction prohibiting Defendants from using its Command and Control Infrastructure to further harm Plaintiff and the general public. A permanent injunction is the only way to afford relief and abate future harm in this case.

Plaintiff duly served Defendants with the Complaint and all pleadings and orders of the

Court in this action in a manner consistent with Due Process and this Court's instructions. Plaintiff serve Defendants by email on July 24, 2020, July 29, 2020 and August 3, 2020, attaching the Complaint, TRO and the foregoing link to all other pleadings, documents and orders in the case and thereafter, by email and publication at the website http://www.dxclegalnotice.com/. Defendants failed to respond and the Clerk of the Court entered default on December 18, 2020. Dkt. No. 35. 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 John Doe Defendants' coordinated cyberattack against DXC. Defendants are the persons responsible for developing a command and control infrastructure comprised of server computers hosting certain Internet domains (*i.e.* websites) through which they directed malicious software to DXC's servers and networks.

Defendants' Method of Attacking DXC's Computers and Networks

Evidence indicates that the defendants operate in the following manner.

The infection process started when an attacker gained unauthorized access to a DXC network that is primarily used by DXC's Xchanging business. Declaration of Mark Hughes ("Hughes Decl.") ¶ 7, Dkt No 3-1.

After gaining access to this network, the attacker installed software known as Cobalt Strike BEACON on workstation computers and servers connected to the network. *Id.* at ¶ 8. The software has capabilities that can be used for malicious activities. *Id.* The attacker installed the software using a technique that manipulates otherwise legitimate processes running on targeted

computers to execute unauthorized code, which is intended to avoid detection by security tools. Once installed, the software deployed a number of "backdoor" files in those computers. *Id.* These backdoor files are used by the attacker-installed software to "beacon" out through the Internet from those systems to the attacker's infrastructure in order to establish Internet connections for further use by the attacker. *Id.* To do this, the attacker-installed software rotates through multiple different domains that are configured in the backdoor files to try to connect to them and then ultimately to the attacker's infrastructure. *Id.* This rotation through multiple domains is intended to avoid interruption (e.g., a domain no longer exists) and evade countermeasures (e.g., access to a domain is blocked in that system). *Id.* The attacker also used a reverse proxy service called Cloudflare to mask the IP address to which traffic to these domains was ultimately connecting. *Id.*

The backdoor files that the attacker deployed on targeted workstation computers and servers were configured to communicate to various subdomains of three (3) attacker-owned domains, as follows:

probes[.]website
probes[.]space
probes[.]site
hyui[.]org

Id. at ¶ 9; Dkt. Nos. 22, 23 and 24; Dkt. No. 27-1 at ¶¶ 3-11.

The attacker was then able to use the connections established through the software backdoors to download and deploy ransomware software on workstation computers and servers in the targeted network, which encrypted the files on them and also created a ransom note file that included a request for payment in exchange for decryption of the files. Hughes Decl. at ¶ 10. The type of ransomware deployed is novel or at least little-known in the security community. *Id.*

Defendants appear to have taken steps to disguise their activities, including software installation techniques designed to avoid detection and using software configured to use multiple domains to avoid interruption and evade countermeasures, as well as masking their ultimate IP address through use of Cloudflare. *Id.* at ¶ 12. Defendants use these domains in an attempt to mask their activity and to attack DXC-owned systems used by DXC and its customers. *Id.* at ¶ 13.

The Court's Injunctions, Defendants' Disregard Of The Injunctions, And Defendants' Continued Harmful Activities Through The Course Of This Case

On July 22, 2020, the Court entered a TRO that disabled Defendants' technical infrastructure used to carry out attacks and to steal information and intellectual property. Dkt. No. 13. On August 3, 2020, the Court entered a Supplemental TRO to take down an additional domain. Dkt. No 23. On August 7, 2020, the Court entered a Preliminary Injunction to ensure that Defendants' infrastructure cannot cause further harm. Dkt. No. 32.

There is evidence that Defendants' disregard of 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. Second, after Defendants' infrastructure was disabled and Defendants were directed to cease their activities the Defendants registered a new domain which indicates that Defendants intentionally have and are likely in the future to intentionally violate any permanent injunction. Dkt. No. 23.

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 its Command and Control 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), and the common law doctrines of trespass to chattels, conversion, and unjust enrichment;

- 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), and the common law doctrines of trespass to chattels, conversion, and unjust enrichment;

III. LEGAL STANDARD

Rule 55 of the Federal Rules of Civil Procedure authorizes the entry of a default judgment when a defendant fails to plead or otherwise defend in accordance with the Federal Rules. *Tweedy v. RCAM Title Loans, LLC*, 611 F. Supp. 2d 603, 605 (W.D. Va. 2009) (citing *United States v. Moradi*, 673 F.2d 725, 727 (4th Cir. 1982)). 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 against a properly served defendant who fails to file a timely responsive pleading." *LPS Default Solutions, Inc. v. Friedman & MacFadyen, P.A.*, 2013 U.S. Dist. LEXIS 108486, at *2-3 (D. Md. Aug. 2, 2013). Default judgment is appropriate when the adversary process has been halted because of an unresponsive party. *SEC v. Lawbaugh*, 359 F. Supp. 2d 418, 421 (D. Md. 2005). Upon default, the well-pled allegations in a complaint as to liability are taken as true. *Id.* Here, the Clerk has entered Defendants' default under Rule 55(a) (Dkt. No. 35), and Defendants have received notice of the same.

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. *Tweedy*, 611 F. Supp. 2d at 605-606 (citing *Faulknier v. Heritage Financial Corp*., 1991 U.S. Dist. LEXIS 15748 (W.D. Va. May 20, 1991) and 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. *E.g.*, *Trs. of the Nat'l Asbestos Workers Pension Fund v. Ideal Insulation, Inc*., 2011 U.S. Dist. LEXIS 124337, at *12 (D. Md. Oct. 27, 2011) (collecting cases). Permanent injunctions depriving cybercrime defendants of their malicious infrastructure, on an ongoing basis in the future, have been entered by this Court in connection with entry of default judgments. *See America Online v. IMS*, 1998 U.S. Dist. LEXIS 20645 (E.D. Va. Dec. 30, 1998) (Brinkema, J.); *Microsoft Corp. v. Doe*, 2015 U.S. Dist. LEXIS 109729 (E.D. Va. Aug. 17, 2015) (O'Grady, J.); *Microsoft Corp. v. Doe*, 2015 U.S. Dist. LEXIS 110145 (E.D. Va. July 20, 2015) (Report and Recommendation); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 46951 (E.D. Va. Apr. 2, 2014) (Brinkema, J.); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398 (E.D. Va. Jan. 6, 2014) (Report and Recommendation).

IV. DISCUSSION

A. Due Process Has Been Satisfied

Plaintiff has served the Complaint, Summons, and all orders and pleadings on Defendants using the methods ordered by the Court under Rule 4(f)(3), including service by email and

publication. Dkt. No. 13 at pp. 7-8. 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., FMAC Loan Receivables v. Dagra,* 228 F.R.D. 531, 534 (E.D. Va. 2005) (acknowledging that courts have readily used Rule 4(f)(3) to authorize international service through non-traditional means, including email); *Mullane v. Central Hanover Bank & Trust Co*., 339 U.S. 306, 314 (1950) (discussing Due Process requirements). 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 when completing the registration process for the domains used in Defendants' command and control infrastructure. *FMAC Loan Receivables,* 228 F.R.D. at 534; *Rio Props., Inc. v. Rio Int'l Interlink*, 284 F.3d 1007, 1014-15 (9th Cir. 2002) ("[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…"); *BP Prods. N. Am., Inc. v. Dagra*, 236 F.R.D. 270, 271-273 (E.D. Va. 2005) (approving notice by publication in two Pakistani newspapers circulated in the defendant's last-known location); *Microsoft Corp. v. John Does 1-27,* Case No. 1:10-cv-156 (E.D. Va. 2010) at Dkt. No. 38 at p. 4 (authorizing service by email and publication in similar action) (Brinkema, J.).

In this case, the email addresses provided by Defendants to the domain registrars, in the course of obtaining services that support Defendants' 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. *See BP Products North Am., Inc.,* 236 F.R.D. at 271. Moreover, Defendants will expect notice regarding their use of the domain registrars' services to operate their 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 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. *See Tweedy*, 611 F. Supp. 2d at 605-606 (applying default factors). 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 and documentary evidence about Defendants' infrastructure. The allegations and evidence in the detailed Complaint and otherwise in the record establish that Defendants' conduct 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), and the common law of trespass to chattels, conversion, and unjust enrichment.

Third, this case involves a matter of substantial public importance. Defendants are

perpetrating serious offenses and civil torts that cause substantial harm to 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 has 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.

Finally, the grounds offered for the entry of a default judgment are clearly established. Plaintiff's application for Default and supporting declaration establish that Defendants have been served. Moreover, the detailed Complaint and the record as a whole establishes Defendants' unlawful conduct and the harm it has caused.

C. Plaintiff Has Adequately Pled 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"), and the common law doctrines of trespass to chattels, conversion, and unjust

enrichment. 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 interstate or foreign commerce or communication." *SecureInfo Corp. v. Telos Corp.*, 387 F. Supp. 2d 593, 608 (E.D. Va. 2005). 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.* (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 gained unauthorized access to a DXC network and installed ransomware software on workstation computers and servers in the targeted network to deceive DXC's customers and to attack DXC's devices. Dkt. No. 1 ¶¶ 19-25. The Complaint alleges damage of more than $5,000 dollars. *Id.* ¶¶ 35. 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. Global Policy Partners, LLC v. Yessin*, 2009 U.S. Dist. LEXIS 112472, *9-13 (E.D. Va. 2009) (accessing computer using credentials that did not belong to defendant was actionable under the CFAA); *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. *See DIRECTV, Inc. v. Benson*, 333 F. Supp. 2d 440, 449 (M.D.N.C. 2004).

The Complaint alleges that DXC's operating system and DXC's customers' computers are facilities through which electronic communication service is provided to DXC's users and customers. Dkt. No. 1 ¶¶ 19-25, 39. Defendants' conduct violates the ECPA because Defendants knowingly and intentionally accessed DXC's operating system, DXC's customers' computers without authorization or in excess of any authorization granted by DXC or any other party. *Id.* ¶ 40. Through this unauthorized access, Defendants intercepted, had access to, obtained and altered authorized access to, wire electronic communications transmitted via DXC's operating system, computers running such software, and DXC's services. *Id.* ¶ 41. Obtaining stored electronic information in this way, without authorization, is a violation of the ECPA. *See Global Policy Partners, LLC*, 686 F. Supp. 2d 631, 635-637 (E.D. Va. 2009) (unauthorized access to emails was actionable under ECPA); *State Analysis, Inc. v. American Fin. Srvcs. Assoc.*, 621 F. Supp. 2d 309, 317-318 (E.D. Va. 2009) (access of data on a computer

without authorization actionable under ECPA). Hacking into a computer and intercepting Internet communications clearly violates the ECPA. *See, e.g., Sharma v. Howard County*, 2013 U.S. Dist. LEXIS 18890, 19 (D. Md. Feb. 12, 2013). Accordingly, Plaintiff properly alleged an ECPA claim and default judgment on this claim is warranted.

Tort Claims. Under Virginia law, the tort of conversion "encompasses any wrongful exercise or assumption of authority . . . over another's goods, depriving him of their possession; and any act of dominion wrongfully exerted over property in denial of the owner's right, or inconsistent with it." *United Leasing Corp. v. Thrift Ins. Corp*., 247 Va. 299, 305 (Va. 1994) (quotation omitted). The related tort of trespass to chattels applies where "personal property of another is used without authorization, but the conversion is not complete." *Dpr Inc. v. Dinsmore*, 82 Va. Cir. 451, 458 (Va. Cir. Ct. 2011) (citations omitted). Here, the Complaint establishes that Defendants exercised dominion and authority over Plaintiff's software and services, converted Plaintiff's property, and were unjustly enriched with ill-gotten benefits reaped from Defendants' infrastructure and its victims. Dkt. No. 1 at ¶¶ 45-47, 53-55, 59-60.

The well-pled allegations in Plaintiff's Complaint, which set forth the elements of each of Plaintiff's claims, are taken as true given Defendants' default. *SEC v. Lawbaugh*, 359 F. Supp. 2d 418, 421 (D. Md. 2005). 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. *See EMI April Music, Inc. v. White*, 618 F. Supp. 2d 497, 509 (E.D. Va. 2009) (citing *Phelps &*

Assocs., LLC v. Galloway, 492 F.3d 532, 543 (4th Cir. 2007)).

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., PBM Prods., LLC v. Mead Johnson & Co.*, 639 F.3d 111, 127 (4th Cir. 2011) (false and misleading representations constituted irreparable harm, and warranted permanent injunction); *Int'l Labor Mgmt. Corp. v. Perez,* 2014 U.S. Dist. LEXIS 57803, 35 (M.D.N.C. Apr. 25, 2014) (damage to "reputation and loss of goodwill constitutes irreparable harm for purposes of injunctive relief") (citing *In Multi-Channel TV Cable Co. v. Charlottesville Quality Cable Operating Co*., 22 F.3d 546 (4th Cir. 1994)); *MicroAire Surgical Instruments, LLC v. Arthrex, Inc.*, 726 F. Supp. 2d 604, 635 (W.D. Va. 2010) ("The loss of goodwill is a well-recognized basis for finding irreparable harm"). The Court previously found that the harm caused to Plaintiff by Defendants, including through unauthorized access to DXC's operating system and the computers, constitutes irreparable harm. Dkt. No. 13 at ¶¶ 3-5. To the extent that Defendants are able to continue to use domains to carry out computer intrusions against DXC and its customers, such irreparable harm would certainly continue in the future.

This finding is consistent with several cases that have concluded that computer malware operations 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., Khepera-Bey v. Santander Consum. USA, Inc*., 2013 U.S. Dist. LEXIS 87641, 13-14 (D. Md. June 21, 2013) ("circumstances[] such as insolvency or unsatisfiability of a money judgment, can show irreparable harm."); *accord Burns v. Dennis-Lambert Invs., Ltd. P'ship*, 2012 Bankr. LEXIS 1107, 9 (Bankr. M.D.N.C. Mar. 15, 2012) ("a preliminary injunction may be appropriate where 'damages may be unobtainable from the defendant because he may become insolvent before final judgment can be entered.'"); *Rudolph v. Beacon Indep. Living LLC*, 2012 U.S. Dist. LEXIS 7075, 5 (W.D.N.C. Jan. 23, 2012) ("Irreparable harm exists here because of Defendant Beacon's continued occupancy of the Facility without paying any rents, particularly in light of the threat of insolvency by one or more Defendants.").

2. <u>The Balance Of Hardships Overwhelmingly Favors An Injunction</u>

Because Defendants are engaged in an illegal scheme to defraud computer users and injure Plaintiff, the balance of equities clearly tips in favor granting an injunction. *See, e.g., PBM Prods.*, 639 F.3d at 127 (where defendant had no legitimate interest in "perpetuating the false and misleading" representations, balance of equities warranted injunction); *US Airways, Inc. v. US Airline Pilots Ass'n,* 813 F. Supp. 2d 710, 736 (W.D.N.C. 2011) (injunction appropriate where, in balance of the equities, denying injunction would result in "enormous disruption and harm" to plaintiff and the public, granting injunction would only require defendant to comply with existing legal duties); *Pesch v. First City Bank of Dallas,* 637 F. Supp.

1539, 1543 (N.D. Tex. 1986) (balance of hardships clearly favors injunction where enjoined activity is illegal). On one side of the scales of equity rests the harm to Plaintiff caused by the Defendants' operation. 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 US Airways,* 13 F. Supp. 2d at 736.

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 CFAA and ECPA. *See, e.g.*, *PBM Prods*., 639 F.3d at 127 (preventing false or misleading representations constitutes a "strong public interest" supporting permanent injunction); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398, 32 (E.D. Va. Jan. 6, 2014) (public interest weighed in favor of injunction to enforce CFAA); *Dish Network LLC v. Parsons,* 2012 U.S. Dist. LEXIS 75386, 8-9 (W.D.N.C. May 30, 2012) (public interest weighed in favor of injunction to enforce ECPA).

Here, Plaintiff requests an injunction that will transfer permanent control of the existing domains to DXC. As a result of such injunction, DXC will be able to protect itself and its customers from the threat of Defendants' operations. Absent the requested injunction, Defendants' existing infrastructure would be released back into Defendants' control, Defendants would be able to establish new malicious domains and associated infrastructure with impunity, and Defendants would be able to use that infrastructure to gain unauthorized access to DXC's operating system and the computers on which such programs and services run and result in unauthorized intrusion into those computers.

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 DXC's control of the existing domains. In particular, the third-party domain registries responsible for administering 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 DXC to compensate the third parties for the assistance rendered.[1] Indeed, Plaintiff has conferred with relevant domain registries and they have no objection to the requested relief.

V. CONCLUSION

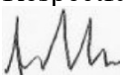
For the reasons set forth in this brief, and based on the Complaint, the evidence submitted in this case and the Court's prior orders, Plaintiff respectfully requests that the Court grant DXC's Motion for Default Judgment and Permanent Injunction.

---

[1] 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. at 174 (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); *United States v. X,* 601 F. Supp. 1039, 1042 (D. Md. 1984) (order to a third party to provide "nonburdensome technical assistance"); *Moore v. Tangipahoa Parish Sch. Bd*., 507 Fed. App'x. 389, 396 (5th Cir. 2013) (unpublished) ("The All Writs Act provides 'power to a federal court to issue such commands . . . as may be necessary or appropriate to effectuate and prevent the frustration of orders it has previously issued in its exercise of jurisdiction otherwise obtained.'") (citing *New York Tel. Co*., 434 U.S. at 172); *In re Application of United States for an Order Authorizing An In-Progress Trace of Wire Commc'ns Over Tel. Facilities*, 616 F.2d 1122, 1129 (9th Cir. 1980) (same); *In re Baldwin-United Corp*., 770 F.2d 328, 338-339 (2d Cir. 1985) ("An important feature of the All-Writs Act is its grant of authority to enjoin and bind non-parties to an action when needed to preserve the court's ability to reach or enforce its decision in a case over which it has proper jurisdiction").

Dated: December 21, 2020

Respectfully submitted,



Julia Milewski (VA Bar No. 82426)
Matthew 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
mwelling@crowell.com

Gabriel M. Ramsey (*pro hac vice*)
Kayvan M. Ghaffari (*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
kghaffari@crowell.com

Attorneys for Plaintiff DXC Technology Company