

control infrastructure away from Defendants and to DXC's control, which will cut communications between Defendants and the targeted DXC devices, thereby halting the criminal activity that is harming DXC. Transfer of the domains to DXC will enable DXC to take steps to remove or disable the Defendants' malicious code on DXC's servers or networks attempting to connect to the domains, thereby mitigating the impact of Defendants' activity.

Ex parte relief is essential. Notice to Defendants would provide them with an opportunity to destroy, move, conceal, or otherwise make inaccessible the instrumentalities they use to direct the operation and the evidence of their unlawful activity. If they learn of the impending action, defendants may attempt to abandon or decrease use of that infrastructure and move to new infrastructure in order to continue efforts to compromise DXC systems. Giving Defendants that opportunity would enable them to continue their illegal activities and render further prosecution of this lawsuit entirely fruitless.

This type of requested *ex parte* relief is not uncommon when disabling an online command and control infrastructure used by unidentified defendants for illegal operations and cybercrime schemes. Courts involving other similar plaintiffs have granted such relief and adopted an approach where:

1. The Court issued a tailored *ex parte* TRO, including provisions sufficient to effectively disable the harmful cybercrime infrastructure, preserve all evidence of its operations and stop the irreparable harm being inflicted on plaintiff;
2. Immediately after implementing the TRO, plaintiff undertook a comprehensive effort to provide notice of the preliminary injunction hearing and to effect service of process on Defendants, including Court-authorized alternate service by email, electronic messaging services, mail, facsimile, publication, and treaty-based means; and
3. After notice, the Court held a preliminary injunction hearing and granted the preliminary injunction in order to ensure that the harm caused by the cybercrime infrastructure would not continue.

See Sophos v. John Does 1-2, No. 1:20-cv-502 (E.D. Va. 2020) (O’Grady, J.).

If the Court grants DXC’s requested relief, immediately upon execution of the TRO, DXC will make a robust effort in accordance with the requirements of due process to provide notice of the preliminary injunction hearing and to serve process on Defendants. DXC will immediately serve the complaint and all papers in this action on Defendants, using known contact information and contact information maintained by domain registrar and registries that host Defendants’ command and control infrastructure.

I. STATEMENT OF FACTS

A. 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.

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

Id. at ¶9.

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. *Id.* 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.

B. Harm to DXC

DXC is a provider of technology-enabled business processing, technology services, and other technology-focused services to customers throughout the world. *Id.* at ¶14. This includes services provided to DXC customers through DXC's Xchanging business. *Id.* DXC has

invested substantial resources in developing high-quality services, as well as building and operating the computer systems used to provide those services in a reliable and highly available manner. *Id.* Due to the high quality and effectiveness of DXC's services and the expenditure of significant resources by DXC to market its services, DXC has generated substantial goodwill with its customers, has established a strong brand, and has developed the DXC and Xchanging names into world-wide symbols that are well-recognized within DXC's channels of trade. *Id.* The activities carried out by the defendants, described above, injure DXC and its reputation, brand and goodwill. *Id.* at ¶15.

DXC is injured because the defendants direct their intrusions to DXC computer systems that are used by DXC to provide services to its customers. *Id.* at ¶16. DXC must respond to customer service inquiries and issues caused by the defendants and must expend substantial resources dealing with the mitigation of the issue and assisting customers to avoid any injury caused by defendants. *Id.* DXC has had to expend substantial resources in an attempt to assist its customers and to prevent the misperception that DXC is the source of damage caused by the defendants. *Id.* For example, DXC must expend resources to remove or otherwise mitigate the impacts of the malicious software used by defendants as discussed above. *Id.*

Customers may incorrectly attribute the negative impact of the defendants to DXC. *Id.* at ¶17. There is a serious risk that defendants' actions will interfere with DXC's business activities and its relationships with its customers. *Id.* Defendants' activities create a serious risk of unwarranted impairment of DXC's goodwill and defendants' activities improperly create perceived risk that interferes with DXC's relationships. *Id.*

Among other things, the defendants install and run software without DXC's or its customers' knowledge or consent, to support the defendants' attacks and to attempt to steal

information. *Id.* at ¶18. The defendants have specifically targeted the DXC-owned systems primarily used by DXC’s Xchanging business to provide services to DXC customers. *Id.* For example, as discussed they execute unauthorized code, deploy unauthorized software and encrypt electronic files, without the consent of DXC or its customers. *Id.*

All of the foregoing activities and circumstances cause injury to DXC. *Id.* ¶19.

II. LEGAL STANDARD

The purpose of a temporary restraining order and preliminary injunction is to prevent irreparable harm during the pendency of a lawsuit and to preserve the court’s ability to render a meaningful judgment on the merits. *United States v. South Carolina*, 720 F.3d 518, 524 (4th Cir. 2013) (citations omitted). “Parties seeking a preliminary injunction must demonstrate that (1) they are likely to succeed on the merits, (2) they are likely to suffer irreparable harm, (3) the balance of hardships tips in their favor, and (4) the injunction is in the public interest.” *Metro. Reg'l Info. Sys. v. Am. Home Realty Network, Inc.*, 722 F.3d 591, 595 (4th Cir. 2013) (citing *Winter v. Natural Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008)).

III. PLAINTIFFS’ REQUESTED RELIEF IS WARRANTED

This matter presents a quintessential case for injunctive relief. Defendants’ conduct causes irreparable harm to DXC and is contrary to the public interest. Every day that passes gives Defendants an opportunity to gain unauthorized access to DXC’s devices and information stored on those devices, and to attempt to expand their illegal operations. Unless enjoined, Defendants will continue to cause irreparable harm to DXC.

A. DXC Is Likely to Succeed on the Merits of Its Claims

Even at this early stage in the proceedings, the record demonstrates that DXC will be able to establish the elements of each of its claims. The evidence in support of DXC’s TRO

Application is based on the diligent work of experienced investigators and is supported by substantial empirical and forensic evidence. Given the strength of DXC’s evidence, the likelihood of success on the merits weighs heavily in favor of granting injunctive relief.

1. Defendants’ Conduct Violates the CFAA

Congress enacted the Computer Fraud and Abuse Act (the “CFAA”) specifically to address computer crime. *See, e.g., Big Rock Sports, LLC v. AcuSport Corp.*, No. 4:08-CV-159-F, 2011 WL 4459189, at *1 (E.D.N.C. Sept. 26, 2011). “Any computer with Internet access [is] subject [to] the statute’s protection.” *Id. Inter alia*, 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.” *See Estes Forwarding Worldwide LLC v. Cuellar*, 239 F. Supp. 3d 918, 926 (E.D. Va. 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 923 (citing 18 U.S.C. § 1030(e)(6)). In order to prosecute a civil claim under the CFAA, a plaintiff must demonstrate loss or damage in excess of \$5,000. The CFAA defines loss as “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or

other consequential damages incurred because of interruption of service.” *Sprint Nextel Corp. v. Simple Cell, Inc.*, No. CIV. CCB-13-617, 2013 WL 3776933, at *6 (D. Md. July 17, 2013) (citing 18 U.S.C. § 1030(e)(8)). “[D]amage . . . means any impairment to the integrity or availability of data, a program, a system, or information.” *Id.* (citing 18 U.S.C. § 1030(e)(11)). The Fourth Circuit has recognized that this “broadly worded provision plainly contemplates consequential damages” such as “costs incurred as part of the response to a CFAA violation, including the investigation of an offense.” *A.V. ex rel. Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 646 (4th Cir. 2009). The CFAA permits plaintiffs to aggregate multiple intrusions or violations for the purposes of meeting the \$5,000 statutory threshold. *See Sprint Nextel Corp.*, 2013 WL 3776933, at *7 (citations omitted).

In sum, in order to prevail on their CFAA claim, DXC must establish that Defendants (1) accessed a protected computer; (2) without authorization or exceeding authorized access; (3) for the purpose of obtaining information or causing transmission of a program or code to the computer, and; (4) resulting in loss or damage in excess of \$5,000. Mark Hughes’ Declaration establishes that Defendants’ conduct satisfies each of these elements. First, each of the devices accessed by the Defendants is, by definition, a protected computer, because only such devices that connect to the Internet can possibly be accessed by Defendants to install their malicious software. *See supra*; 18 U.S.C. § 1030(e)(2)(B) (defining “protected computer” as a computer “used in interstate or foreign commerce or communication”). Second, each device into which Defendants have intruded by installing malicious software has been accessed without authorization, as such activity has been without DXC’s or its customers’ knowledge or consent. *See supra*. Third, Defendants damage DXC and its devices—*inter alia*—by impairing the integrity of DXC’s devices. *See supra*. Finally, the amount of harm caused by the Defendants

exceeds \$5,000. *See supra*.

Defendants' conduct is precisely the type of activity that the Computer Fraud and Abuse Act is designed to prevent. *See, e.g., Physicians Interactive v. Lathian Sys., Inc.*, No. CA 03-1193-A, 2003 WL 23018270, at *1 (E.D. Va. Dec. 5, 2003) (granting TRO and preliminary injunction under CFAA where defendant hacked into a computer and stole confidential information); *Glob. Policy Partners, LLC v. Yessin*, 686 F. Supp. 2d 631 (E.D. Va. 2009) (accessing computer using credentials that did not belong to defendant actionable under the CFAA); *see also United States v. Phillips*, 477 F.3d 215, 219 (5th Cir. 2007) (noting that CFAA is concerned with "outside hackers who break into a computer") (citations to legislative history omitted). Thus, DXC is likely to succeed on the merits of its CFAA claim.

2. Defendants' Conduct Violates the ECPA

The Electronic Communications Privacy Act 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). DXC's servers and its licensed operating system at end user computers are facilities through which electronic communication services are provided. Defendants' conduct violates the ECPA because Defendants break into computing devices and computer networks with the direct intention of acquiring the contents of sensitive communications be they e-mails, voicemails, or other communications types. Defendants use software, installed without authorization on compromised computers to do so. Obtaining stored electronic information in this way, without authorization, is a violation of the Electronic Communications Privacy Act. *See Council on Am.-Islamic Relations v. Gaubatz*, 667 F. Supp. 2d 67, 71-73 (D.D.C. 2009) (granting preliminary

injunction in case where plaintiff brought ECPA claims after defendant removed 12,000 internal, sensitive documents including emails and other documents and made video and audio recordings of private meetings and published this information); *Microsoft Corp.*, 2014 WL 1338677, at *7 (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 plaintiff’s 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”). Thus, DXC is likely to succeed on the merits of its Electronic Communications Privacy Act claim.

3. Defendants’ Conduct is Tortious

Defendants’ conduct is tortious under the common law doctrines of conversion, trespass to chattels, and unfair competition.

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.” *Microsoft Corp. v. Does 1-2*, No. 1:16CV993, 2017 WL 5163363, at *5 (E.D. Va. Aug. 1, 2017), *report and recommendation adopted*, No. 1:16-CV-00993 (GBL/TCB), 2017 WL 3605317 (E.D. Va. Aug. 22, 2017); *see also Ground Zero Museum Workshop v. Wilson*, 813 F. Supp. 2d 678, 697 (D. Md. 2011) (holding defendant liable for conversion where defendant replaced current version of plaintiffs’ website with former version, because such action effectively “dispossessed [plaintiff] of the chattel;” *i.e.*, its website). The related tort of trespass to chattels—sometimes referred to as “the little brother of conversion”—applies where personal property of another is used without authorization, but the conversion is not complete. *Id.*; *see also Vines v. Branch*, 418 S.E.2d 890, 894 (1992).

Here, Defendants exercised dominion and authority over DXC's property by intruding into its servers and by injecting changes into DXC's software that fundamentally altered important functions of the software on those servers. These acts deprived DXC of its right to control the content, functionality, and nature of its servers, software and services. District courts in the Fourth Circuit have recognized that computer hacking can amount to tortious conduct under the doctrines of conversion and trespass to chattels. *See supra*; *see also Microsoft Corp. v. Does 1-18*, No. 1:13CV139 LMB/TCB, 2014 WL 1338677, at *9 (E.D. Va. Apr. 2, 2014) ("The unauthorized intrusion into an individual's computer system through hacking, malware, or even unwanted communications supports actions under these claims"); *Microsoft Corp. v. John Does 1-8*, No. 1:14-CV-811, 2015 WL 4937441, at *12 (E.D. Va. Aug. 17, 2015).

Further, Defendants' conduct amounts to unjust enrichment because plaintiff has demonstrated that (1) plaintiff conferred a benefit on the defendants; (2) defendants had knowledge of the conferring of the benefit; and, (3) defendants acceptance or retention of the benefit under the circumstances "render it inequitable for the defendant to retain the benefit without paying for its value." *Microsoft Corp. v. John Does 1-8*, 2015 WL 4937441, at *12. For example, unjust enrichment has been found where a defendant "[w]ithout authorization ... used [plaintiff's] servers, networks, [and] operating system, to operate and propagate" a botnet, profited from such activity and thus it "would be inequitable for defendant to retain the benefits from this unlawful scheme." *Microsoft Corp.*, 2014 WL 1338677, at *10. The same is true here.

Thus, DXC is likely to succeed on the merits of its common law claims.

B. Defendants' Conduct Causes Irreparable Harm

It is well-established that intrusions into protected computers by cybercriminals, which they threaten to attempt to repeat on an ongoing basis, constitutes irreparable harm. *See Microsoft Corp. v. John Does 1-2*, No. 1:16-cv-993 (GBL/TCB), 2016 U.S. Dist. LEXIS 199109, at **3-4 (E.D. Va. Aug. 12, 2016) (“intentionally accessing and sending malicious software, code, and instructions to the protected computers” in order to install “malicious code” and to “attack and compromise the security of those computers” constituted threat of irreparable harm).

Here, the Defendants threaten to irreparably harm DXC by virtue of their continued attempts to direct their intrusions to DXC’s devices. DXC must expend substantial resources to engage with customers and block the malicious software on an ongoing basis. All of this constitutes irreparable harm. *See Multi-Channel TV Cable Co. v. Charlottesville Quality Cable Operating Co.*, 22 F.3d 546, 552 (4th Cir. 1994) (“[W]hen the failure to grant preliminary relief creates the possibility of permanent loss of customers to a competitor or the loss of goodwill, the irreparable injury prong is satisfied.”), *abrogated on other grounds, Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 24 (2008). In addition, Defendants are causing monetary harm that is unlikely to ever be compensated—even after final judgment—because Defendants are elusive cybercriminals whom DXC is unlikely to be able to enforce judgments against.

“[C]ircumstances[] such as insolvency or unsatisfiability of a money judgment, can show irreparable harm.” *Khepera-Bey v. Santander Consumer USA, Inc.*, No. CIV. WDQ-11-1269, 2013 WL 3199746, at *4 (D. Md. June 21, 2013); *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*, No. 3:11-CR-00617-W, 2012 WL 181439, at *2 (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.”).

C. The Balance of Equities Strongly Favor Injunctive Relief

Because Defendants are engaged in an illegal scheme to injure DXC and to compromise its devices, the balance of equities clearly tips in favor granting an injunction. *See, e.g., US Airways, Inc. v. US Airline Pilots Ass’n*, 813 F. Supp. 2d 710, 736 (W.D.N.C. 2011); *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 DXC caused by the Defendants, while on the other side of the scales, Defendants can claim no legally cognizable harm because an injunction would only require Defendants to cease illegal activities. *US Airways*, 13 F. Supp. 2d at 736.

D. The Public Interest Favors an Injunction

It is clear that an injunction would serve the public interest here. Every day that passes, there is the possibility that Defendants will attempt to intrude into new DXC devices in order to access the computing resources and information on those devices. These ongoing likely attempts are contrary to the public interest, which thus weighs in favor of granting injunctive relief. This is because the requested injunctive relief both enables DXC to mitigate impact to its devices by taking control of the domains at issue and to halt Defendants’ ability to continue their activities through existing infrastructure. Moreover, the public interest is clearly served by enforcing statutes designed to protect the public, such as the CFAA. *See, e.g., Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398, at *32 (E.D. Va. Jan. 6, 2014) (public interest weighed in favor of injunction to enforce CFAA).

Notably, numerous courts that have confronted requests for injunctive relief targeted at disabling malicious domains used by cyber criminals have ordered transfer of such domains away from the malicious actors. *See Microsoft Corp. v. John Does 1-8*, No. 1:14-cv-811, 2015 WL 4937441, at *12 (E.D. Va. Aug. 17, 2015); *Sophos v. John Does 1-2*, Case No. 1:20-cv-000502 (E.D. Va. May 1, 2020) (granting preliminary injunction order). DXC respectfully submits that the same result is warranted here.

E. **The All Writs Act Authorizes the Court to Direct Third Parties to Perform Acts Necessary to Avoid Frustration of the Requested Relief**

DXC's Proposed Order directs that the third parties whose infrastructure Defendants rely on to operate the malicious domains reasonably cooperate to effectuate the order. Critically, these third parties are the only entities within the United States that can effectively disable command and control infrastructure, and thus their cooperation is necessary.

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). The Supreme Court has recognized that narrow direction to third parties necessary to effect the implementation of a court order is authorized by the All Writs Act:

The power conferred by the Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice, and encompasses even those who have not taken any affirmative action to hinder justice.

United States v. New York Tel. Co., 434 U.S. 159, 174 (1977) (citations omitted) (order to telephone company to assist in implementation of a pen register warrant was authorized under the All Writs Act).

Numerous Courts of Appeal have emphasized the importance of such authority of federal courts to enforce their own orders. *See 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*, 616 F.2d 1122, 1129 (9th Cir. 1980) (same; noting of *New York Tel. Co.*, 434 U.S. at 175, “the Court made the commonsense observation that, without the participation of the telephone company, ‘there is no conceivable way in which the surveillance authorized could have been successfully accomplished”); *In re Baldwin-United Corp.*, 770 F.2d 328, 338-39 (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”; “[The Court does] not believe that Rule 65 was intended to impose such a limit on the court’s authority provided by the All-Writs Act to protect its ability to render a binding judgment.”);

Numerous courts have utilized the authority of the All Writs Act to order third party technical infrastructure providers to provide tailored assistance in the context of malicious online conduct, where such was necessary to effectuate a court order and preserve the court’s jurisdiction. *See Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398 at *30 (invoking All Writs act and granting relief similar to that requested herein); *United States v. X*, 601 F. Supp. 1039, 1042 (D. Md. 1984) (All Writs Act permits the district court to order a third party to provide “nonburdensome technical assistance” in aid of valid warrant); *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).

Requiring these third parties to reasonably assist in the execution of this order will not offend due process as the Proposed Order (1) requires only minimal assistance from the third

parties in executing the order (acts that they would take in the ordinary course of their operations), (2) requires that it be implemented with the least degree of interference with the normal operation of third parties, (3) does not deprive the third parties of any tangible or significant property interests and (4) requires DXC to compensate the third parties for the assistance rendered. If, in the implementation of the Proposed Order, any third party wishes to bring an issue to the attention of the Court, DXC will bring it immediately. The third parties will have an opportunity to be heard at the preliminary injunction hearing, which must occur shortly after the execution of the Proposed Order. Fed. R. Civ. P. 65(b)(2). The directions to third parties in the Proposed Order are thus narrow, satisfy due process, and are necessary to effect the requested relief and ensure that the relief is not rendered fruitless.

F. An Ex Parte TRO and Preliminary Injunction Is the Only Effective Means of Relief, and Alternative Service Is Warranted Under the Circumstances

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

If notice is given prior to issuance of a TRO, it is likely that Defendants will be able to quickly mount an alternate command and control structure, in order to continue targeting DXC and its devices, causing such devices to begin to communicate through that alternate structure before the TRO can have any remedial effects. Thus, providing notice of the requested TRO will

undoubtedly facilitate efforts by Defendants to defend their operations. It is well established that *ex parte* relief is appropriate under circumstances such as the instant case, where notice would render the requested relief ineffective. *See, e.g., AllscriptsMisys, LLC v. Am. Dig. Networks, LLC*, 1:10-cv-00111, 2010 U.S. Dist. LEXIS 4450, at *2 (D. Md. Jan. 20, 2010) (granting an *ex parte* TRO where “Defendant may dissipate the funds and/or take action to render it difficult to recover funds.”); *Crosby v. Petromed, Inc.*, No. CV-09-5055-EFS, 2009 WL 2432322, at *2 (E.D. Wash. Aug. 6, 2009) (granting *ex parte* TRO as “notice to Defendants of this TRO request could result in further injury or damage to Plaintiffs....”); *AT&T Broadband v. Tech Commc’ns, Inc.* 381 F.3d 1309, 1319-20 (11th Cir. 2004) (affirming *ex parte* search and seizure order to seize contraband technical equipment, given evidence that in the past defendants and persons similarly situated had secreted evidence once notice given); *Little Tor Auto Ctr. v. Exxon Co.*, 822 F. Supp. 141, 143 (S.D.N.Y. 1993) (*ex parte* TRO appropriate where contraband “may be destroyed as soon as notice is given”); *In re Vuitton Et Fils S.A.*, 606 F.2d 1, 4-5 (2d Cir. 1979) (per curiam) (holding that notice prior to issuing TRO was not necessary where notice would “serve only to render fruitless further prosecution of the action”; prior experience taught that once one member of the counterfeiting enterprise received notice, contraband would be transferred to another unknown counterfeiter, perpetuating the harm and rendering judicial efforts pointless).

Similarly, in *FTC v. Pricewert LLC*, Case No. 09-2407 (N.D. Cal.), the district court issued an *ex parte* TRO suspending Internet connectivity of a company enabling botnet activity and other illegal computer-related conduct on the basis that “Defendant is likely to relocate the harmful and malicious code it hosts and/or warn its criminal clientele of this action if informed of the [plaintiff’s] action.” Exs. 8-9 to Declaration of Matthew Welling (“Welling Decl.”).

Moreover, the court in *Dell* issued an *ex parte* TRO against domain registrants where persons similarly situated had previously concealed such conduct and disregarded court orders by, *inter alia*, using fictitious businesses, personal names, and shell entities to hide their activities. *Dell*, 2007 WL 6862341, at *4. In *Dell*, the Court explicitly found that where, as in the instant case, Defendants' scheme is "in electronic form and subject to quick, easy, untraceable destruction by Defendants," *ex parte* relief is particularly warranted. *Id.* at *2.

To ensure due process, immediately upon entry of the requested *ex parte* TRO, DXC will undertake extraordinary efforts to effect formal and informal notice of the preliminary injunction hearing to Defendants and to serve the complaint.

DXC Will Provide Notice By E-mail, Facsimile And Mail: DXC has identified email addresses, mailing addresses and/or facsimile numbers provided by Defendants, and will further identify such contact information pursuant to the terms of the requested TRO. Welling Decl. at ¶¶ 6-8. DXC will provide notice of the preliminary injunction hearing and will effect service of the Complaint by immediately sending the same pleadings described above to the e-mail addresses, facsimile numbers and mailing addresses that Defendants provided to the registrars and registries. *Id.* When Defendants registered for domain names and IP addresses, they agreed not to engage in abuse such as that at issue in this case and agreed that notice of disputes regarding hosting could be provided to them by sending complaints to the e-mail, facsimile and mail addresses provided by them. *Id.* ¶ 7.

DXC Will Provide Notice To Defendants By Publication: DXC will notify Defendants of the preliminary injunction hearing and the Complaint against their misconduct by publishing the materials on a centrally located, publicly accessible source on the Internet for a period of 6 months. *Id.* ¶ 10.

DXC Will Provide Notice By Personal Delivery And Treaty If Possible: If valid physical addresses of Defendants can be identified, DXC will notify Defendants and serve process upon them by personal delivery or through the Hague Convention on service of process or similar treaty-based means. *Id.* ¶¶ 12-13.

Notice and service by the foregoing means satisfy due process; are appropriate, sufficient, and reasonable to apprise Defendants of this action; and are necessary under the circumstances. DXC hereby formally requests that the Court approve and order the alternative means of service discussed above.

First, legal notice and service by e-mail, facsimile, mail and publication satisfies due process as these means are reasonably calculated, in light of the circumstances, to apprise the interested parties of the TRO, the preliminary injunction hearing, and the lawsuit. *See Mullane v. Cent. Hanover Bank & Tr. Co.*, 339 U.S. 306, 314 (1950). Such methods are also authorized under Federal Rule of Civil Procedure 4(f)(3), which allows a party to serve defendants by means not prohibited by international agreement. The methods of notice and service proposed by DXC have been approved in other cases involving international defendants attempting to evade authorities. *See e.g., Rio Properties, Inc. v. Rio Int’l. Interlink*, 284 F.3d 1007, 1014-15 (9th Cir. 2002) (authorizing service by e-mail upon an international defendant); *Microsoft Corp. v. Does 1-18*, No. 1:13-cv-139 LMB/TCB, 2014 WL 1338677, at *3 (E.D. Va. Apr. 2, 2014) (finding service was proper where plaintiff sent “copies of the original Complaint, Russian translations, a link to all pleadings, and the TRO notice language to all email addresses associated with the Bamital botnet command and control domains” and “published in English and Russian the Complaint, Amended Complaint, Summons, and all orders and pleadings in this action at the publicly available website www.noticeofpleadings.com”) (citing Fed.R.Civ.P.

4(f)(3)); *FMAC Loan Receivables v. Dagra*, 228 F.R.D. 531, 535-36 (E.D. Va. 2005) (acknowledging that courts have readily used Rule 4(f)(3) to authorize international service through non-traditional means); *BP Products N. Am., Inc. v Dagra*, 236 F.R.D. 270, 271-73 (E.D. Va. 2006) (approving notice by publication); *AllscriptsMisys, LLC v. Am. Dig. Networks, LLC*, 2010 U.S. Dist. LEXIS 4450, at *3 (D. Md. 2010) (granting *ex parte* TRO and order prompting “notice of this Order and Temporary Restraining Order [] can be effected by telephone, electronic means, mail or delivery services.”).

Such service is particularly warranted in cases such as this involving Internet-based misconduct, carried out by international defendants, causing immediate, irreparable harm. As the Ninth Circuit observed:

[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 e-mail—the method of communication which [Defendant] utilizes and prefers. In addition, e-mail was the only court-ordered method of service aimed directly and instantly at [Defendant] ... Indeed, when faced with an international e-business scofflaw, playing hide-and-seek with the federal court, e-mail may be the only means of effecting service of process.

Rio Properties, Inc., 284 F.3d at 1018. Notably, *Rio Properties* has been followed in the Fourth Circuit. See *FMAC Loan Receivables*, 228 F.R.D. at 534 (following *Rio*); *BP Products N. Am., Inc. v. Dagra*, 232 F.R.D. 263, 264 (E.D. Va. 2005) (same); *Williams v. Adver. Sex LLC*, 231 F.R.D. 483, 486 (N.D. W. Va. 2005) (“The Fourth Circuit Court of Appeals has not addressed this issue. Therefore, in the absence of any controlling authority in this circuit, the Court adopts the reasoning of the Ninth Circuit in *Rio Properties, Inc. . . .*”).

In this case, the e-mail addresses provided by Defendants domain registrar and registries and to the hosting companies, in the course of obtaining services that support the Defendants’ cybercrime infrastructure, are likely to be the most accurate and viable contact information and means of notice and service. Moreover, Defendants will expect notice regarding their use of the

domain registrar's and registries' services to operate their infrastructure by those means, as Defendants agreed to such in their agreements. *See Nat'l Equip. Rental, Ltd. v. Szukhent*, 375 U.S. 311, 315-16 (1964) ("And it is settled ... that parties to a contract may agree in advance to submit to the jurisdiction of a given court, to permit notice to be served by the opposing party, or even to waive notice altogether."). For these reasons, notice and service by e-mail and publication are warranted and necessary here.¹

For all of the foregoing reasons, DXC respectfully requests that the Court enter the requested TRO and Order to Show Cause why a preliminary injunction should not issue, and further order that the means of notice of the preliminary injunction hearing and service of the Complaint set forth herein meet Fed. R. Civ. P. 4(f)(3), satisfy due process, and are reasonably calculated to notify Defendants of this action.


II. CONCLUSION

For the reasons set forth herein, DXC respectfully requests that this Court grant its motion for a TRO and order to show cause regarding a preliminary injunction. DXC further respectfully requests that the Court permit notice of the preliminary injunction hearing and service of the Complaint by alternative means.

¹ Additionally, if the physical addressees provided by Defendants to hosting companies turn out to be false and Defendants' whereabouts are unknown, the Hague Convention will not apply in any event and alternative means of service, such as email and publication, would be appropriate for that reason as well. *See BP Products.*, 236 F.R.D. at 271 ("The Hague Convention does not apply in cases where the address of the foreign party to be served is unknown.").

Dated: July 20, 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 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