

**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

**DECLARATION OF GABRIEL M. RAMSEY IN SUPPORT OF
DXC’S REQUEST FOR ENTRY OF DEFAULT**

I, Gabriel M. Ramsey, declare as follow:

1. I am an attorney admitted to practice in the State of California. I am a partner at the law firm of Crowell & Moring LLP, counsel of record for Plaintiff DXC Technology Company (“DXC”). I make this declaration in support of DXC’s Request for Entry of Default. I have personal knowledge of the facts set forth in this declaration and, if called to testify as a witness, could and would testify to the following under oath.

A. Defendants Have Not Responded To This Action Or Otherwise Objected To The Relief Requested In This Action

2. As described more fully below, John Doe Defendants 1-2 (“Defendants”) have been properly served the Complaint, summons, and all orders, pleadings and evidence in this action pursuant to the means authorized by the Court in the Temporary Restraining Order (Dkt. No. 13), Supplemental TRO (Dkt. No. 23), and Preliminary Injunction Order (Dkt. No. 32), and Defendants have failed to plead or otherwise defend the action.

3. As of December 16, 2020, I have not been contacted by any of the Defendants

regarding this case or at all. I have also conferred with Plaintiff, who confirms that neither DXC, nor any party associated with it, have been contacted by any of the Defendants regarding this case or at all. Defendants have not objected to the relief obtained in the Temporary Restraining Order or the Preliminary Injunction Order. Defendants have not objected to or disputed any pleading, declaration, fact, evidence or submission in this case.

4. The 21-day time for Defendants to respond to the complaint under Fed. R. Civ. P. 12 has expired, as Defendants were served with the complaint and all pleadings on July 24, 2020, July 29, 2020 and August 3, 2020 via email and publication and were subsequently served with the preliminary injunction on August 7, 2020. Upon information and belief, the Defendants against whom a notation of default is sought are not infants or incompetent persons. I base this conclusion on the fact that Defendants have engaged in sophisticated acts of computer intrusion and theft of sensitive information from computer networks and have operated and procured sophisticated cybercrime infrastructure. I have also seen no indication that Defendants are absent or have failed to file responsive pleadings due to present military service.

B. Service Of Process And Notice Upon Defendants

1. Defendants Are Aware Of This Proceeding Given The Impact Of The TRO And Preliminary Injunction Orders

5. I submit that it is most reasonable to conclude that Defendants are aware of this proceeding given the significant impact of the TRO and preliminary injunction orders on their operations, in combination with the steps DXC took to serve process by email and through publication, discussed below.

6. As attested in the Declaration of Mark Hughes (Dkt. No. 3-1 ¶¶ 23-25 and Dkt. No. 27-1 ¶¶ 3-4) following execution of the TRO and preliminary injunction orders, the subject Internet domains that comprised Defendants' command and control infrastructure were

transferred to DXC's control. As attested, this mechanism was designed to interrupt Defendants' attacks by cutting communications between Defendants' existing command and control infrastructure and the ransomware used in the attack on DXC-owned computer system. *Id.* Given the obvious impact on the infrastructure, I conclude that Defendants are very likely to be aware of that impact and to be aware of the fact that the instant proceeding is the cause of that impact.

C. **Service By Internet Publication**

7. DXC has served process by Internet publication, as authorized by the TRO and Preliminary Injunction Order. The Court has authorized service by Internet publication, as follows: "the Complaint may be served by any means authorized by law, including . . . publishing notice on a publicly available Internet website." Dkt. No. 13 at pp. 7-8.

8. I personally oversaw service of process by publication, including each of the following actions, on behalf of DXC.

9. Beginning on July 24, 2020, I published the Complaint, summons, TRO and all associated pleadings, declaration and evidence on the publicly available website <http://www.dxclegalnotice.com/>. Thereafter, I published the Supplemental TRO and Preliminary Injunction Order and all other pleadings, declarations, evidence, orders and other submissions filed with the Court in this action on the publicly available website <http://www.dxclegalnotice.com/>. All pleadings and orders filed with the Court have been made available on that website throughout the case.

10. I also included prominently at the top of the website, the following text:

"Plaintiff DXC Technology Company has sued Defendants John Does 1-2 associated with the Internet domains listed in the documents attached herein. DXC alleges that Defendants have violated Federal and state law by hosting a cybercriminal operation through these

Internet domains, causing unlawful intrusion into DXC's computers and intellectual property violations to the injury of DXC. DXC seeks a preliminary injunction directing the registries associated with these Internet domains to transfer control of them to DXC and to take steps to prevent Defendants from accessing these domains. DXC seeks a permanent injunction, other equitable relief and damages. Full copies of the pleading documents are available at www.DXClegalnotice.com.

NOTICE TO DEFENDANT: READ THESE PAPERS

CAREFULLY! You must "appear" in this case or the other side will win automatically. To "appear" you must file with the court a legal document called a "motion" or "answer." The "motion" or "answer" must be given to the court clerk or administrator within 21 days of the date of first publication specified herein. It must be in proper form and have proof of service on the DXC's attorneys, Gabriel M. Ramsey at Crowell & Moring, 3 Embarcadero Center, 26th Floor, San Francisco, CA 94111. If you have questions, you should consult with your own attorney immediately."

11. A link to the foregoing website was included in each service of process email sent to Defendants at the email addresses determined to be associated with Defendants' domains. Attached hereto as **Exhibit 1** is a true and correct copy of a screenshot of the publicly available website <http://www.dxclegalnotice.com/>.

D. Service By Email

12. DXC has served process through email, as authorized by the TRO and Preliminary Injunction Order. The Court has authorized service by email, as follows: "the Complaint may be served by any means authorized by law, including (1) transmission by email . . . to the contact information provided by Defendants to Defendants' domain registrars and/or hosting companies." Dkt. No. 13 at pp. 7-8.

13. Through DXC's pre-filing investigation, its investigators and attorneys at Crowell & Moring LLP gathered contact information, particularly email addresses, associated with Defendants' domains. Defendants provided these email addresses to domain registrars when completing the registration process for the domains used in Defendants' command and control

infrastructure. I used this contact information to serve Defendants by email.

14. In this case, the email addresses provided by Defendants to the domain registrars are the most accurate and viable contact information and means of notice and service. I have personally researched in detail the identifying information and mailing addresses used in the registration of the domains used by Defendants, as discussed further below. In each case, my investigation has shown that Defendants provided to the domain registrars false or stolen names, addresses, facsimile numbers and telephone numbers. However, in each case, Defendants provided an operational, active email address to the domain registrar. Defendants will have expected notice regarding their use of the domains by the email addresses that they provided to their domain registrars. For example, as set forth in the Declaration of Matthew Welling at Dkt. No. 3-2 ¶¶ 15-29, ICANN domain registration policies require Defendants to provide accurate email contact information to registrars and the registrars use such information to provide notice of complaints and to send other account-related communications about the domain, including communications which result in suspension or cancellation of the domain registration.

15. Given that Defendants connected to the infected victim computers through these domains, it was crucial for them to remain vigilant as to any change of the domains' status, and the email addresses associated with the domains are the means by which they did so. For example, during the course of discovery in this action, I received subpoena responses from the email providers associated with Defendants' email addresses which show that the domain registrars often sent communications, including renewal and billing notices and other communications to Defendants at the email addresses they had provided in association with the domains. Since Defendants were able to maintain the domains active until the execution of this Court's TRO, Supplemental TRO, and Preliminary Injunction Order, it follows that Defendants

monitored the email accounts to maintain use of the domain registrars' services.

16. I served copies of the Complaint, TRO, Supplemental TRO, Preliminary Injunction Order, and all other pleadings, declarations, evidence, orders and other submissions in this action, by attaching those documents as PDF files to emails sent to the email addresses associated with the domains used by Defendants. In each such email, I included a link to the website <http://www.dxclegalnotice.com/>, at which the pleadings, declarations, evidence and orders filed in this action could also be accessed.

17. I have served the Complaint, TRO, Supplemental TRO, Preliminary Injunction Order, and all other pleadings, declarations, evidence, orders and other submissions in this action, by sending them to the following email addresses used by the Defendants:

probeswork666@gmail.com
fb9612e372434681a12a34685d6de6e7.protect@whoisguard.com

18. In particular, on July 24, 2020, July 29, 2020 and August 3, 2020, I served the Defendants by sending an email to Defendants, attaching the Complaint, TRO and the foregoing link to all other pleadings, documents and orders in the case. In these initial emails that I sent to Defendants, I included the following text:

“Plaintiff DXC Technology Company has sued Defendants John Does 1-2 associated with the Internet domains listed in the documents attached herein. DXC alleges that Defendants have violated Federal and state law by hosting a cybercriminal operation through these Internet domains, causing unlawful intrusion into DXC’s computers and intellectual property violations to the injury of DXC. DXC seeks a preliminary injunction directing the registries associated with these Internet domains to transfer control of them to DXC and to take steps to prevent Defendants from accessing these domains. DXC seeks a permanent injunction, other equitable relief and damages. Full copies of the pleading documents are available at www.DXClegalnotice.com.

NOTICE TO DEFENDANT: READ THESE PAPERS CAREFULLY! You must “appear” in this case or the other side will win automatically. To “appear” you must file with the court a legal document called a “motion” or “answer.” The “motion” or “answer” must be given to the court clerk or

administrator within 21 days of the date of first publication specified herein. It must be in proper form and have proof of service on the DXC's attorneys, Gabriel M. Ramsey at Crowell & Moring, 3 Embarcadero Center, 26th Floor, San Francisco, CA 94111. If you have questions, you should consult with your own attorney immediately."

19. On August 3, 2020, I served the Supplemental TRO, by sending an email attaching that order to Defendants, and again including the foregoing language.

20. On August 7, 2020, I served the Preliminary Injunction Order, by sending an email attaching that order to Defendants, and again including the foregoing language.

21. Despite this robust notice and service, the Defendants have not contacted me, anyone at my firm, DXC, nor any other party associated with DXC. Despite notice and service, Defendants have not objected to the relief obtained in the Temporary Restraining Order, Supplemental TRO, and the Preliminary Injunction Order. Despite notice and service, Defendants have not objected to or disputed any pleading, declaration, fact, evidence or submission in this case.

22. I used an email tracking service to monitor whether the service emails that I sent to Defendants were opened. The service reported that the emails were specifically opened by Defendants on the following date and time:

July 24, 2020 at 16:03:21pm (UTC -8:00)

E. Attempted Notice And Service By Mail Or Personal Delivery

23. I have investigated each physical mailing address listed in the public registration information associated with the domains used by the Defendants and in the records regarding those domains obtained during discovery. This information was fabricated by Defendants. These addresses reflected: (1) incomplete addresses, such as only the names of cities without further detail, (2) addresses that are simply artificial and do not exist at all, and (3) street names

that exist but not properly correlated to other address information.

24. From the foregoing, I conclude that the email addresses associated with the domains and, which are described further above, are the most viable way to communicate with the Defendants in this action. As noted above, Defendants provided these email addresses when registering the domains used in the command and control infrastructure of their cybercrime operations making it likely that Defendants at least monitor messages sent to those addresses.

F. DXC Has Made Substantial, But Unsuccessful, Efforts To Discover And Investigate Defendants' Particular Identities, Thus The Foregoing Email Information Remains The Best Means To Serve Process In This Case

25. On behalf of DXC, I endeavored to identify additional contact information through which Defendants could be served, as well as more specific identities. Over the course of Plaintiff's investigation, pursuant to the Court's discovery order, I served a total of thirteen subpoenas to domain registrars and hosting companies ("collectively ISPs"), payment processors, and communications companies in an effort to obtain additional information regarding Defendants' identities.

26. These discovery efforts yielded various names, addresses and payment information. Further investigation revealed that the names, addresses, and credit card information used by Defendants were fake or stolen. Defendants also made numerous payments using anonymous Bitcoin payments that are not associated with any particular identity.

27. I identified several hosting companies involved with Defendants' infrastructure and from discovery to those sources learned and examined IP addresses used to create, host and log into that relevant infrastructure. Defendants, however, used sophisticated techniques and services designed to conceal their actual IP address and location, and to proxy their communications through third-party computers. Thus, it has not been possible to identify Defendants with any greater particularity through these means either.

28. I have continued to pursue discovery leads and received subpoena responses within the last week, which coincided with the close of discovery on December 7, 2020.

29. 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, I have been unable to specifically and definitively determine the "real" names and physical addresses of Defendants, at which they might be served by personal service.

30. Although Defendants' true identities remain unknown, discovery efforts have confirmed a connection to Russia, and Plaintiff, at the time of this Court's order, was assessing its options with respect to this information and potential avenues for further investigation or relief in or with respect to that country.

31. During my investigation of email addresses, I encountered only instances in which Defendants had used free email services in jurisdictions which have no reciprocal discovery means with the United States. During my investigation of domain and hosting account information, I discovered that Defendants logged into these accounts from IP addresses that were determined to be proxies. Based on my experience investigating cybercrime matters, I am aware that the sole purpose of such proxy services is to allow Internet users to anonymously use the Internet, without divulging the user's IP address. These proxy computers and services cycle Internet access through a large number of globally distributed IP addresses, thereby concealing the location of the user accessing the Internet through the service. For example, the Internet

user's connection to the Internet may be through a first IP address and ordinarily that is what would be displayed when a legitimate user is accessing an email account. However, by using the proxy service, Defendants' access will reflect the IP address of the proxy computer, rather than the user's actual connection. Often these services "chain" together multiple proxy computers, to make it nearly impossible to trace the original IP address of the user.

32. In particular, my investigation revealed that Defendants used anonymous VPN services or networks and/or the "The Onion Router" (aka "Tor") networks, which are collectively designed to and have the effect of concealing the source IP address by encrypting the traffic and routing it through multiple, random intermediate computers. I determined this by either looking up the IP addresses in publicly available repositories of known Tor nodes, or by sending subpoenas and informal requests to the operators of the IP addresses and receiving responses that they were such nodes. The result is that login IP addresses seen in email account, registrar and hosting company records are from random intermediate machines in scores of countries (and given the operation of anonymous VPN and Tor, those intermediate machines often have numerous other intermediate machines between the login IP and Defendants' ultimate source IP). Thus, Defendants were able to conceal their identities, source IP addresses and physical locations.

33. I have carried out every reasonable effort and have used every tool, technique and information source available to me to further specifically identify Defendants' true identities and physical locations. I conclude that I have exhausted my ability to investigate Defendants' true identities using civil discovery tools, despite my best efforts and the exercise of reasonable diligence to determine Defendants' identities.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct to the best of my knowledge. Executed on this 16th day of December, 2020, in San Francisco, California.

A handwritten signature in black ink, appearing to read "Gabriel M. Ramsey", written in a cursive style.

Gabriel M. Ramsey

Exhibit 1

Date of First Publication: July 24, 2020


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

DXC TECHNOLOGY COMPANY,)	
a Nevada corporation,)	
)	
Plaintiff,)	Civil Action No: 1:20-cv-814
v.)	
)	
JOHN DOES 1-2,)	
)	
)	
Defendants.)	
)	
)	

Plaintiff DXC Technology Company has sued Defendants John Does 1-2 associated with the Internet domains listed in the documents attached herein. DXC alleges that Defendants have violated Federal and state law by hosting a cybercriminal operation through these Internet domains, causing unlawful intrusion into DXC’s computers and intellectual property violations to the injury of DXC. DXC seeks a preliminary injunction directing the registries associated with these Internet domains to transfer control of them to DXC and to take steps to prevent Defendants from accessing these domains. DXC seeks a permanent injunction, other equitable relief and damages. Full copies of the pleading documents are available at www.DXClegalnotice.com (<https://www.DXClegalnotice.com>).

NOTICE TO DEFENDANT: READ THESE PAPERS CAREFULLY! You must “appear” in this case or the other side will win automatically. To “appear” you must file with the court a legal document called a “motion” or “answer.” The “motion” or “answer” must be given to the court clerk or administrator within 21 days of the date of first publication specified herein. It must be in proper form and have proof of service on the DXC’s attorneys, Gabriel M. Ramsey at Crowell & Moring, 3 Embarcadero Center, 26th Floor, San Francisco, CA 94111. If you have questions, you should consult with your own attorney immediately.


CIVIL COVER SHEET

Civil Cover Sheet ([https://dxclegalnotice.com/files/Civil Cover Sheet/DXC - Civil Cover Sheet.pdf](https://dxclegalnotice.com/files/Civil%20Cover%20Sheet/DXC%20-%20Civil%20Cover%20Sheet.pdf)) 


COMPLAINT

Complaint (<https://dxclegalnotice.com/files/Complaint/Complaint.pdf>) 

APPEARANCES

Notice of Appearance of Julia Milewski (<https://dxclegalnotice.com/files/Appearances/Notice of Appearance for Milewski.pdf>) 

Motion for Pro Hac Vice for Gabriel Ramsey (<https://dxclegalnotice.com/files/Appearances/Ramsey PHV.pdf>) 


Motion for Pro Hac Vice for Matthew Welling (<https://dxclegalnotice.com/files/Appearances/Welling PHV.pdf>) 

Motion for Pro Hac Vice for Kayvan Ghaffari (<https://dxclegalnotice.com/files/Appearances/Ghaffari PHV.pdf>) 


RULE 7.1 STATEMENT


Rule 7.1 Statement (<https://dxclegalnotice.com/files/Rule 7.1/Rule 7.1.pdf>) 


EX PARTE APPLICATION FOR EMERGENCY TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION


Ex Parte Application for Emergency Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction (<https://dxclegalnotice.com/files/TRO/TRO Motion.pdf>) 


Brief In Support of Ex Parte Application for Emergency Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction (<https://dxclegalnotice.com/files/TRO/TRO Brief.pdf>) 

Declaration of Mark Hughes In Support of Ex Parte Application for Emergency Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction (<https://dxclegalnotice.com/files/TRO/Hughes Decl.pdf>) 

Declaration Matthew Welling In Support of Ex Parte Application for Emergency Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction (<https://dxclegalnotice.com/files/TRO/Welling Decl with Exhibits.pdf>) 


Proposed Order In Support of Ex Parte Application for Emergency Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction (<https://dxclegalnotice.com/files/TRO/TRO Proposed Order Updated.pdf>) 

Notice of Telephonic Hearing on Ex Parte Application for Emergency Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction (<https://dxclegalnotice.com/files/TRO/Notice of Telephonic Hearing.pdf>) 


Notice in Support of DXC's Ex Parte Application for Emergency Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction (<https://dxclegalnotice.com/files/TRO/Notice in Support of TRO.pdf>) 

MOTION FOR PROTECTIVE ORDER

Motion for Protective Order (<https://dxclegalnotice.com/files/Protective Order/PO Motion.pdf>) 

Brief In Support of Motion for Protective Order (<https://dxclegalnotice.com/files/Protective Order/PO Brief.pdf>) 


Declaration of Gabriel Ramsey (<https://dxclegalnotice.com/files/Protective Order/Ramsey Decl ISO PO.pdf>) 


Proposed Order In Support of Motion for Protective Order (https://dxclegalnotice.com/files/Protective Order/2020-08-06 ECF 28_Motion for Limited Auth to Conduct Discovery to ID & Serve Doe Defendants.pdf) 


COURT ORDERS


Motion for Temporary Restraining Order (<https://dxclegalnotice.com/files/Court Orders/TRO Order.pdf>) 


Motion to Seal (<https://dxclegalnotice.com/files/Court Orders/DXC-Order Granting Motion to Seal.pdf>) 


Motion for Pro Hac Vice for Gabriel Ramsey (https://dxclegalnotice.com/files/Court Orders/2020-07-29 ECF 18_Order Granting Motion for Admission to Appear PHV_Gabriel Ramsey.pdf) 

Motion for Pro Hac Vice for Matthew Welling (https://dxclegalnotice.com/files/Court Orders/2020-07-29 ECF 16_Order Granting Motion for Admission to Appear PHV_Matthew Welling.pdf) 


Motion for Pro Hac Vice for Kayvan Ghaffari (https://dxclegalnotice.com/files/Court Orders/2020-07-29 ECF 17_Order Granting Motion for Admission to Appear PHV_Kayvan Ghaffari.pdf) 


Supplemental Temporary Restraining Order (<https://dxclegalnotice.com/files/Court Orders/DXC-Supplemental TRO Order.pdf>) 

Motion for Limited Authority to Conduct Discovery Necessary to Identify and Serve Doe Defendants (<https://dxclegalnotice.com/files/Court Orders/2020-08-7 ECF 31 Order Granting Doe Discovery.pdf>) 

Directing to File Entry of Default and Motion for Default Judgment (<https://dxclegalnotice.com/files/Court Orders/DXC-Order 12-15-20.pdf>) 

NOTICE

Notice of Supplemental Authority In Support of Temporary Restraining Order (<https://dxclegalnotice.com/files/Notice/DXC-Notice of Supp App A.pdf>) 


Notice of Supplemental Declaration of Mark Hughes In Support of Order to Show Cause re Preliminary Injunction (https://dxclegalnotice.com/files/Notice/2020-08-06 ECF 27_Notice of Suppl Decl of Mark Hughes ISO Order to Show Cause re PI.pdf) 


PRELIMINARY INJUNCTION


Proposed Preliminary Injunction Order (<https://dxclegalnotice.com/files/Preliminary Injunction/DXC-PI Order 8-3.pdf>) 

MOTION FOR LIMITED AUTHORITY TO CONDUCT DISCOVERY NECESSARY TO IDENTIFY AND SERVE DOE DEFENDANTS


Motion (https://dxclegalnotice.com/files/Motion_For_Limited/2020-08-7 ECF 31 Order Granting Doe Discovery.pdf) 

Brief In Support (https://dxclegalnotice.com/files/Motion_For_Limited/2020-08-06 ECF 29_Brief ISO Motion for Limited Auth to Conduct Discovery to ID & Serve Doe Defendants.pdf) 

Proposed Order (https://dxclegalnotice.com/files/Motion_For_Limited/2020-08-06 ECF 28-1_Proposed Order.pdf) 

Notice re Hearing (https://dxclegalnotice.com/files/Motion_For_Limited/2020-08-06 ECF 30_Notice of Waiver of Hearing on DXC's Doe Discovery Motion.pdf) 

MISCELLANEOUS

Confirmation of Surety Bond (https://dxclegalnotice.com/files/Miscellaneous/2020-08-05 ECF 25_DXC-Surety Bond Confirmation.pdf) 

Contact Us

If you wish to contact us by e-mail, fax, phone or letter please contact us at:

Gabriel Ramsey
Crowell & Moring LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111

Telephone: +1 (415) 365-7207
Facsimile: +1 (415) 986-2827
Email: gramsey@crowell.com (<mailto:gramsey@crowell.com>)