IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Microsoft Corporation, a Washington State Corporation, NGO-ISAC, a New York State Non-Profit Organization, Plaintiffs, v. John Does 1-2, Controlling A Computer Network and Thereby Injuring Plaintiff and Its Customers, Defendants.	Civil Action No. 1:24-cv-02719-RC **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5.1**

PLAINTIFFS' MOTION FOR PROTECTIVE ORDER TEMPORARILY SEALING DOCUMENTS RE PLAINTIFFS' MOTION TO SUPPLEMENT PRELIMINARY INJUNCTION ORDER

Pursuant to Fed. R. Civ. P. 26(c)(1) and Local Civil Rule 5, Plaintiffs Microsoft Corp. ("Microsoft") and NGO Information Sharing and Analysis Center ("NGO-ISAC") hereby move for a protective order temporarily sealing the pleadings associated with the First *Ex Parte* Motion to Supplement the Preliminary Injunction Order, and the following documents in particular, filed by Plaintiffs in this action;

1. Plaintiffs' First *Ex Parte* Motion to Supplement the Preliminary Injunction Order;
2. Memorandum in Support of Plaintiffs' First *Ex Parte* Motion to Supplement the Preliminary Injunction Order;
3. Declaration of Sean Ensz In Support of Plaintiffs' First *Ex Parte* Motion to Supplement Preliminary Injunction Order and associated appendices;
4. [Proposed] Order Granting Plaintiffs' First *Ex Parte* Motion to Supplement Preliminary Injunction Order;

5. The instant Motion for Protective Order Temporarily Sealing Documents;
6. Memorandum in Support of Plaintiffs' Motion for Protective Order Temporarily Sealing Documents;
7. The declaration of Jeffrey L. Poston in Support of Motion for Protective Order Temporarily Sealing Documents; and
8. [Proposed] Order Granting Plaintiffs' Motion for Protective Order Temporarily Sealing Documents

Plaintiffs respectfully request that these materials be sealed pending execution of the ex parte relief sought in Plaintiffs' First *Ex Parte* Motion to Supplement the Preliminary Injunction Order, in particular the disabling of the domains set forth in Appendix A to the proposed First Supplemental Preliminary Injunction Order. Plaintiffs respectfully request that upon the execution of the portion of the Order disabling the domains in Appendix A to the First Supplemental Preliminary Injunction Order, the foregoing documents be filed on the public docket. Upon execution of that *ex parte* relief, Plaintiffs will file with the Clerk of the Court a Notice that the Supplemental Preliminary Injunction Order has been executed. Plaintiffs further request that upon execution of the Supplemental Preliminary Injunction Order, Plaintiffs be permitted to disclose such materials as it deems necessary to commence its efforts to provide Defendants notice of any further hearings and service of pleadings associated with the instant First *Ex Parte* Motion to Supplement the Preliminary Injunction Order. Plaintiffs respectfully request that should the Court decide not to grant the *ex parte* temporary relief requested in Plaintiffs' First *Ex Parte* Motion to Supplement the Preliminary Injunction Order, that the materials be sealed indefinitely.

Dated: November 5, 2024

/s/Jeffrey L. Poston

Jeffrey L. Poston (DC Bar No. 426178)
Garylene Javier (*pro hac vice*)
JPoston@crowell.com
GJavier@crowell.com
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington, DC 20004

Anna Z. Saber (*pro hac vice*)
ASaber@crowell.com
CROWELL & MORING LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111

Counsel for Plaintiffs Microsoft Corporation and NGO-ISAC

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Microsoft Corporation, a Washington State Corporation, NGO-ISAC, a New York State Non-Profit Organization, Plaintiffs, v. John Does 1-2, Controlling A Computer Network and Thereby Injuring Plaintiffs and Its Customers, Defendants.	Civil Action No. 1:24-cv-02719-RC **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5.1**

MEMORANDUM IN SUPPORT OF PLAINTIFFS' MOTION FOR PROTECTIVE ORDER TEMPORARILY SEALING DOCUMENTS RE PLAINTIFFS' MOTION TO SUPPLEMENT PRELIMINARY INJUNCTION ORDER

Plaintiffs submit the following memorandum in support of their Motion for a Protective Order Temporarily Sealing Documents.

BACKGROUND

Plaintiffs Microsoft Corporation ("Microsoft") and NGO Information Sharing and Analysis Center ("NGO-ISAC") previously obtained a TRO and Preliminary Injunction to prevent the activities of John Doe Defendants 1 and 2 (collectively "Defendants") who are engaged in harmful and malicious Internet activities directed at Microsoft, its customers, NGO-ISAC, its member organizations, and the general public. Since the Court granted the Preliminary Injunction, the Star Blizzard Defendants have attempted to rebuild their technical infrastructure to continue their criminal operation. Plaintiffs have filed an *Ex Parte* Motion to Supplement the Preliminary Injunction Order, whereby Plaintiffs seek *ex parte* relief to disable the recently registered domains set forth in **Appendix A** to the Proposed Order,

mitigate against the irreparable harm caused by the Star Blizzard Defendants criminal conduct. Plaintiffs seek this relief under seal, because advance public disclosure or notice of the requested relief would allow the Star Blizzard Defendants to evade such relief and further prosecution of this action, thereby perpetuating the irreparable harm at issue. The reasons for sealing are the same reasons that Plaintiffs previously put forth in connection with their TRO Application. Dkt. 4-1 at 32-33. Therefore, Plaintiffs request that the First *Ex Parte* Motion to Supplement the Preliminary Injunction Order and associated pleadings be sealed pending execution of the *ex parte* relief sought in Plaintiffs' First Supplemental Preliminary Injunction Order, in particular disabling of the domains set forth in **Appendix A** to the Proposed Order. Plaintiffs' requested sealing order is narrowly tailored to impose the least restriction on the public's right of access to information as possible. Plaintiffs request that all sealed documents be immediately unsealed upon execution of the portion of the Order disabling the domains set forth in **Appendix A** to the Proposed Order. As soon as that relief is executed, Plaintiffs will file a notice of execution and will seek unsealing of the documents, such that all papers will be made available on the public docket.

ARGUMENT

The right of access to court records is not absolute. *Nixon v. Warner Commc'ns, Inc.*, 435 U.S. 589, 597-98 (1978). Although both common law and the First Amendment afford the public a qualified right of access to judicial proceedings, *In re Fort Totten Metrorail Cases*, 960 F. Supp. 2d 2, 5 (D.C. Cir. 2013), the D.C. Circuit has expressed doubts about whether the First Amendment right of access applies outside of the criminal context. *SEC v. Am. Int'l Grp.*, 712 F.3d 1, 5 (D.C. Cir. 2013); *Ctr. for Nat'l Sec. Studies v. DOJ*, 331 F.3d 918, 935 (D.C. Cir. 2003); *In re Reporters*

Comm. for Freedom of the Press, 773 F.2d 1325, 1337 (D.C. Cir. 1985) (Scalia, J.) (doubting that the benefits of open criminal trials inure to civil suits between private parties).

Competing interests may outweigh the public's common law right of access to judicial records. *United States v. Hubbard*, 650 F.2d 293, 317–22 (D.C. Cir. 1980). Indeed, "[a] district court has authority to seal and unseal documents as part of its 'supervisory power over its own records and files.'" *United States v. Ring*, 47 F. Supp. 3d 38, 40 (D.D.C. 2014) (quoting *Nixon v. Warner Commc'ns, Inc.*, 435 U.S. 589, 598 (1978)); *In re Nat'l Broad. Co.*, 653 F.2d 609, 613 (D.C. Cir. 1981) ("Because of the difficulties inherent in formulating a broad yet clear rule to govern the variety of situations in which the right of access must be reconciled with legitimate countervailing public or private interests, the decision as to access is one which rests in the sound discretion of the trial court.").

Under District of D.C. law, the district court should weigh the following when presented with a motion to seal or unseal: "(1) the need for public access to the documents at issue; (2) the extent of previous public access to the documents; (3) the fact that someone has objected to disclosure, and the identity of that person; (4) the strength of any property and privacy interests asserted; (5) the possibility of prejudice to those opposing disclosure; and (6) the purposes for which the documents were introduced during the judicial proceedings." *Hubbard*, 650 F.2d at 317-22; *Metlife, Inc. v. Fin. Stability Oversight Council*, 865 F.3d 661, 666 (D.C. Cir. 2017) (Garland, C.J.) ("[T]he Hubbard test has consistently served as our lodestar because it ensures that we fully account for the various public and private interests at stake.").

The Federal Rules of Civil Procedure also recognize the important public and judicial interest in protecting confidential business information. *See* Fed. R. Civ. P. 26(c)(1)(G) (empowering courts to order "that a trade secret or other confidential research, development, or

commercial information not be revealed or be revealed only in a specified way"). Likewise, Supreme Court and D.C. Circuit authority recognize the necessity of non-public ex parte proceedings. *See Granny Goose Foods, Inc. v. Teamsters,* 415 U.S. 423, 439, 94 S. Ct. 1113 (1974) ("Ex parte temporary restraining orders are no doubt necessary in certain circumstances..."); *Carroll v. President and Com'rs of Princess Anne*, 393 U.S. 175, 180 (1968) ("There is a place in our jurisprudence for ex parte issuance, without notice, of temporary restraining orders."); *Omar v. Harvey*, 2006 WL 286861, at *1 (D.D.C. Feb. 6, 2006) (holding that an ex parte restraining order is appropriate where plaintiff demonstrates notice would render fruitless further prosecution of the action); *Council on American-Islamic Relations v. Gaubatz*, 667 F. Supp. 2d 67, 75 (D.D.C. Nov. 3, 2009) (noting that ex parte restraining orders may be appropriate in circumstances where notice is impossible).

If notice is given prior to issuance of the Supplemental Preliminary Injunction Order, it is likely that the Star Blizzard Defendants will be able to quickly mount an alternate command and control structure and direct the vast majority of the infiltrated computers to begin to communicate through that alternate structure before the TRO can have any remedial effects. Thus, public disclosure of this filing would undermine the relief sought by Plaintiffs. *See* Dkt. No. 4-2 ¶¶ 57-62; Declaration of Sean Ensz In Support of Plaintiffs' First *Ex Parte* Motion to Supplement Preliminary Injunction Order ¶¶ 17-18. To effectively disable the Star Blizzard infrastructure it is necessary to seal the pleadings. This need to seal the pleadings is paramount over any competing public interest to have immediate access to the information Plaintiffs request to be sealed. If the papers are not sealed, there is a substantial risk that the Star Blizzard Defendants would destroy evidence because they are sophisticated cybercriminals with technical expertise to hide their identities. *Id.* Given Plaintiffs' actions against the Star Blizzard Defendants in this case, even

disclosing that Plaintiffs has filed this case and is seeking to takedown the infrastructure of these Star Blizzard Defendants gives the Star Blizzard Defendants the opportunity to change their command and control infrastructure,

Here, there is specific evidence that the Star Blizzard Defendants will attempt to move the infrastructure if given notice, as the Star Blizzard Defendants have persistently changed infrastructure once it becomes known to the security community, in order to stay ahead of cybersecurity counter-measures. Dkt. No. 4-2 ¶¶ 60-61. Accordingly, granting *ex parte* relief while keeping the pleadings temporarily under seal is appropriate. Indeed, district courts have previously granted similar relief in cases brought by Plaintiffs to halt similarly situated cybercriminal operations.

The harm that would be caused by the public filing of Plaintiffs' First *Ex Parte* Motion to Supplement the Preliminary Injunction Order would far outweigh the public's right to access that information. There is no need for the public to have immediate access to the First *Ex Parte* Motiom to Supplement the Preliminary Injunction Order and supporting documents while Plaintiffs are seeking *ex parte* relief with respect to the domains in **Appendix A** to the Proposed Order, which will only be effective if these materials remain under seal. Applying the balancing test set forth in governing law demonstrates that Plaintiffs' interest in obtaining effective relief outweigh any immediate public right to disclosure.

Plaintiffs only seek to seal such information for a limited period of time, until after effective the domains identified in **Appendix A** have been transferred to Microsoft. After such point, sealing will no longer be necessary, and Plaintiffs will immediately commence efforts to provide the Star Blizzard Defendants notice of future hearings and service of related pleadings—at which point, all documents will be unsealed and the public will be given full access to these proceedings.

Plaintiffs, upon execution of the *ex parte* relief disabling the domains in **Appendix A** to the Proposed Order, will file with the Clerk of the Court a Notice that the temporary restraining order has been executed. The Clerk of the Court may then file all documents related to this request on the public docket.

Should, however, the Court decide not to grant the *ex parte* relief Plaintiffs request, Plaintiffs ask that such materials remain sealed for an indefinite period, as public disclosure or notice absent the *ex parte* relief requested would facilitate the Star Blizzard Defendants' harmful and malicious Internet activities.

Given the limited period of sealing as an alternative that balances the public interest in access with Plaintiffs' important interests in maintaining these materials under seal for a brief period of time, granting the instant request to seal is warranted and consistent with the legal framework for addressing this issue.

Dated: November 5, 2024

/s/ Jeffrey L. Poston

Jeffrey L. Poston (DC Bar No. 426178
Garylene Javier (*pro hac vice*)
JPoston@crowell.com
GJavier@crowell.com
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington, DC 20004

Anna Z. Saber (*pro hac vice*)
ASaber@crowell.com
CROWELL & MORING LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111

Counsel for Plaintiffs Microsoft Corporation and NGO-ISAC

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Microsoft Corporation, a Washington State Corporation, NGO-ISAC, a New York State Non-Profit Organization, Plaintiffs, v. John Does 1-2, Controlling A Computer Network and Thereby Injuring Plaintiff and Its Customers, Defendants.	Civil Action No. 1:24-cv-02719-RC **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5.1**

DECLARATION OF JEFFREY L. POSTON IN SUPPORT OF MOTION FOR PROTECTIVE ORDER TEMPORARILY SEALING DOCUMENTS

I, Jeffrey L. Poston, declare as follow:

1. I am an attorney admitted to practice in the District of Columbia. I am a partner at the law firm of Crowell & Moring LLP ("Crowell"), counsel of record for Plaintiffs Microsoft Corporation and NGO-ISAC in this matter. I make this declaration in support of Plaintiffs' Motion for a Protective Order Temporarily Sealing Documents. 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.

2. This case arises out of the harmful and malicious Internet activities of Defendants John Does 1 and 2 (collectively "Defendants"). I am informed and on that basis believe that the Star Blizzard Defendants are sophisticated, Russia-based cybercriminals who specialize in stealing sensitive information from computer networks. I am informed and on that basis believe that the Star Blizzard Defendants orchestrate a comprehensive spear phishing

campaign, make unauthorized access to Plaintiffs' services and software, hack into a target's computer network and email systems, steal login credentials, gain perpetual access to the email accounts, and then exfiltrate sensitive information from them.

3. I am informed and believe that, for reasons explained in detail in the Declaration of Sean Ensz In Support of Plaintiffs' First *Ex Parte* Motion to Supplement Preliminary Injunction Order and the Declaration of Sean Ensz In Support of Plaintiffs' *Ex Parte* Application For Temporary Restraining Order (Dkt. No. 4-2) permitting the Star Blizzard Defendants to learn of these proceedings prior to execution of the temporary *ex parte* relief sought in Plaintiffs' First *Ex Parte* Motion to Supplement Preliminary Injunction Order—in particular the portion to disable the domains in Appendix A to that Order—would preclude Plaintiffs' ability to obtain effective relief against the Star Blizzard Defendants. This is because the Star Blizzard Defendants are highly sophisticated cybercriminals capable of quickly adapting the command and control infrastructure used to perpetrate the Star Blizzard Defendants' unlawful conduct in order to overcome Plaintiffs' remediation efforts.

4. I am informed and believe that, absent a protective order, there is a substantial risk that the Star Blizzard Defendants will learn of these proceedings before the *ex parte* relief to disable the domains in Appendix A to the Supplemental Preliminary Injunction Order can be affected and will take steps to evade the relief sought.

5. Over the past decade, my colleagues and I have been involved in prosecuting over a dozen similar cases against similarly situated cybercriminal organizations. These cases all involved similar litigation strategies and claims and have involved John Doe defendants conducting illegal activities through identifiable but movable online command and control infrastructures similar to that used by the Star Blizzard Defendants in this action. In several of

those cases, Microsoft observed defendants also immediately act to attempt to defy and evade the court's order as soon as they detected legal action being taken against them.

6. Thus, given our past experience with cases with very similar circumstance as those here, it is my belief that even disclosing that Plaintiffs has requested a Supplemental Preliminary Injunction Order to disable the domains at Appendix A to that order gives the Star Blizzard Defendants the opportunity to adapt the command and control infrastructure so that they can continue to perpetrate their unlawful conduct. For this reason, Plaintiffs respectfully requests that all documents filed in this case be temporarily sealed.

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 5th day of November 2024, in Washington, D.C.

/s/ Jeffrey L. Poston
Jeffrey L. Poston