UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC, *Plaintiff,* v. DOES 1–25, *Defendants.*	Civil Action No.:

DECLARATION OF LAURA HARRIS IN SUPPORT OF PLAINTIFF'S MOTION FOR AN *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

I, Laura Harris, hereby declare and state as follows:

1. I am a partner with the law firm of King & Spalding LLP and counsel of record for Plaintiff Google LLC. I am a member in good standing of the bar of the State of New York. I make this declaration in support of Google's Motion for an *Ex Parte* Temporary Restraining Order and Order to Show Cause ("TRO Motion"). I make this declaration of my own personal knowledge and, if called as a witness, I could and would testify competently to the truth of the matters set forth herein.

2. This Court may issue a temporary restraining order without notice to Defendants if "the movant's attorney certifies in writing any efforts made to give notice and the reasons why it should not be required." Fed. R. Civ. P. 65(b)(1)(B). The committee notes to the rule and case law in this district clarify that a TRO without notice may also issue in the absence of efforts to give notice if notice would frustrate the valid purpose of the relief being sought. *See* Fed. R. Civ. P. 65 committee notes to 2001 amendment. I submit this declaration because Google has not provided Defendants with notice of the filing of this action or Google's TRO Motion for the reasons provided below. I certify that the necessity for this emergency hearing arises from the circumstances of this case and not from a lack of diligence on Google's part.

I. Basis For *Ex Parte* TRO Motion

3. Google seeks an *ex parte* temporary restraining order so that it may disrupt Defendants' operation of a far-reaching criminal enterprise (the "Outsider Enterprise" or "Enterprise") that engages in phishing attacks to steal personal and financial information for use in perpetrating cybercrimes, including selling compromised financial information to other cybercriminals.

4. As described in the memorandum of law accompanying Google's Motion and supporting documents, the Outsider Enterprise has developed a software called "Outsider" that the Enterprise leverages to create and deploy large-scale phishing attacks. The software includes templates for fraudulent websites, features designed to evade detection, and lead victims to believe they are dealing with legitimate businesses. *E.g.*, Declaration of NAXO ("NAXO Declaration" or "NAXO Decl.") ¶¶ 22, 30–32, 66, 77.

5. The Outsider Enterprise continues to create new, fraudulent websites every day that bear Google's trademarks and are causing irreparable harm to Google, device users, and the public. For example:

a. The Enterprise uses the Outsider software to create fraudulent websites that can collect victims' financial and personal information. Those sites often use Google logos to resemble legitimate sites. *Id.* ¶¶ 37, 60, 77. Duped by this resemblance, victims will then enter their personal financial information, like credit card or bank account information.

b. The Outsider Enterprise also collects and stores victims' information. *Id.* ¶¶ 9, 90. The Enterprise can then exploit that information themselves or sell the information to other cybercriminals. *Id.* ¶¶ 6, 123, 133.

6. Certain domains have been identified as phishing websites used by the Outsider Enterprise. Those domains are listed in **Appendix A** and **Appendix C** to the NAXO Declaration.

7. To disrupt the Outsider Schemes and the Enterprise behind it, Google has developed a disruption plan that seeks to shut down the domains used by Outsider and disable the servers the Enterprise uses to control its software. To suspend the infrastructure on which the Enterprise relies, Google must act quickly and coordinate with several registrars and web-hosting companies.

8. It is critical to implement this plan without notice to Defendants. With advance notice of these disruption efforts, Defendants could and likely would simply move their infrastructure to new domains or servers, in order to continue their criminal activity, conceal evidence, and frustrate efforts to disrupt their wrongdoing.

9. I have been informed that Google employees investigating Outsider, including Google's CyberCrime Investigation Group, have attempted to identify the true identities of all responsible Defendants but have been unable to do so.

10. This is not surprising to me. Based on my experience on prior similar matters and on Google's research, Defendants likely provided contact information to web-hosting companies during the domain-name registration process, which could potentially include mailing addresses, email addresses, and telephone numbers. In my experience, cybercriminals generally provide fake mailing addresses to registrars and web-hosting companies, but are more likely to provide real email addresses to ensure they receive any notifications regarding service disruptions, registration expiration, or other issues tied to the continued operation of their domains.

11. In past cases against foreign cybercriminals involved in similar phishing schemes, the defendants have submitted fake mailing addresses to registrars and web-hosting companies. *See, e.g.*, Harris Declaration ¶ 13, *Google LLC v. Does 1-25*, No. 25-cv-10440 (S.D.N.Y. Dec. 17, 2025), Dkt. 28 ("Our inquiry concluded that in nearly every case, the addresses produced by the registrars are fictional. Many lack critical information, such as street numbers, street names, or even the country where the address is purportedly located. Others are a mishmash of gibberish."). Indeed, Google has been unable to verify any addresses associated with phishing defendants in those cases despite extensive investigation. *Id.* ¶¶ 12–26 (detailing Google's efforts to verify foreign defendants' addresses, including by "(1) hiring a cyber investigation firm to pursue an

extensive investigation into defendants, (2) seeking the disclosure of addresses associated with defendants from domain registrars, and (3) attempting test mailings and other means of testing the accuracy of the address obtained").

12. Google has not attempted to provide notice of its Motion to Defendants and should not be required to provide notice at this time.

13. As discussed more fully in Google's memorandum of law, Google is likely to prevail on the merits of this case and hold the Outsider Enterprise liable for its violations of federal law. Defendants are operating a worldwide criminal enterprise using the Outsider software; they are using technology that can be easily concealed, transported, and destroyed; and they have inflicted and are continuing to inflict harm on personal users and Google in the process. Without immediate, *ex parte* injunctive relief, Defendants will likely be able to evade any court-ordered efforts to disrupt the Outsider Enterprise by destroying business records, modifying or destroying the Outsider software, and otherwise transporting or concealing evidence of the Enterprise's malicious and criminal activity. For these reasons, there is good cause for this Court to grant the requested relief without providing advance notice to Defendants.

II. Notice and Service of Process to Defendants

14. On behalf of Google, King & Spalding intends to attempt to provide notice of the pleadings, TRO Motion and supporting papers, and any preliminary injunction hearing to Defendants under Federal Rule of Civil Procedure 4(f)(3), which permits service by any court-ordered means "not prohibited by international agreement." Specifically, and if approved by the Court, King & Spalding plans to serve Defendants via (1) website publication, which King & Spalding will keep active for a period of six months; and (2) email, using any information Google

receives through its disruption efforts, its investigation, and from web-hosting companies who may have addresses linked to domain names created to host phishing sites.

15. Defendants are believed to reside in China, but they go to great lengths to conceal their identities and locations, and their true locations remain unknown.

16. Google anticipates that it will not be able to identify Defendants' addresses even with reasonable diligence. Google has already conducted its own investigation into Defendants' activities and has hired a cyber investigation firm to pursue its own extensive investigation. *See, e.g.*, Declaration of Google ¶¶ 3, 22; NAXO Decl. ¶¶ 6–7.

17. If the Court grants the requested *ex parte* TRO, Google will serve the TRO on domain registries to obtain Defendants' addresses. Google will investigate these addresses with reasonable diligence, conducting a comprehensive review to determine their validity. The results of this investigation will determine whether additional methods of service of process are appropriate or required.

18. If Defendants' physical addresses become known and verifiable, Google will promptly inform the Court and take all necessary steps to ensure service consistent with applicable international agreements in advance of any hearing on a preliminary injunction.

In accordance with 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Executed on June 12, 2026, in New York, New York.

/s/ Laura Harris
Laura Harris