UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

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

PLAINTIFF'S MEMORANDUM OF LAW
IN SUPPORT OF ITS MOTION TO FILE APPENDICES A AND C UNDER SEAL
AND REDACT CERTAIN INVESTIGATIVE AND IDENTIFYING INFORMATION

Plaintiff Google LLC has filed a Complaint and a Motion for an *Ex Parte* Temporary Restraining Order and Order to Show Cause to disrupt a global criminal enterprise that has stolen personal and financial information from more than 100,000 victims and exploits the trust and goodwill associated with Google's brand. Due to the surreptitious nature of Defendants' cybercriminal activity, Google does not yet know the true identities of the Doe Defendants, sued as Does 1–25. Google seeks *ex parte* relief in its TRO to disable the internet infrastructure listed in appendices to its motion, *see* Appendices A and C to the NAXO Decl. in Supp. of Pl.'s Mot. for TRO and Order to Show Cause, and to mitigate the irreparable harm caused by Defendants' criminal conduct. Further evidence in support of Google's filings is set forth in declarations submitted by a Google employee (the "Google Declaration" or "Google Decl.") and an investigator at the digital forensics firm NAXO (the "NAXO Declaration or NAXO Decl.").

Google respectfully requests leave under Federal Rule of Civil Procedure 5.2(d)–(e) to: (1) redact information identifying its declarants in order to protect those individuals' privacy interests and prevent harassment or retaliation from Defendants; (2) redact portions of the Google

Declaration and NAXO Declaration detailing investigative processes, including references to a specific domain, digital fingerprints, and email addresses connected to that domain; and (3) file Appendices A and C to the NAXO Declaration under seal and redact references to the contents of Appendices A and C.

The public has a "general right to inspect and copy public records and documents, including judicial records and documents." *Kahle v. Cargill, Inc.*, 2024 WL 5168057, at *1 (S.D.N.Y. Dec. 19, 2024) (quoting *Nixon v. Warner Commc'ns, Inc.*, 435 U.S. 589, 597 (1978)). However, "[w]hen a district court initially considers a request to seal a file or to approve or take other protective measures, it enjoys considerable discretion in determining whether good cause exists to overcome the presumption of open access to [filed] documents." *Fournier v. Erickson*, 242 F. Supp. 2d 318, 341 (S.D.N.Y. 2003) (quoting *Geller v. Branic Int'l Realty Corp.*, 212 F.3d 734, 738 (2d Cir. 2000)). "Documents may be sealed 'only with specific, on-the-record findings that sealing is necessary to preserve higher values and only if the sealing order is narrowly tailored to achieve that aim.'" *Cunningham v. Cornell Univ.*, 2019 WL 10892081, at *1 (S.D.N.Y. Sept. 27, 2019) (quoting *Brown v. Maxwell*, 929 F.3d 41, 47 (2d Cir. 2019)).

First, good cause exists to redact the names of the Google and NAXO declarants to protect these individuals' privacy interests and prevent harassment or retaliation from Defendants. Google's requested relief seeks to effectuate a major disruption of Defendants' phishing schemes and, as a result, their financial interests. Defendants may seek to retaliate. This concern is not merely hypothetical: Defendants in a different Google case targeting a cybercriminal scheme attempted to contact members of Google's legal team by email and in person. *See Google LLC v. Does 1–25*, No. 25-cv-4503 (S.D.N.Y. July 11, 2025), Dkt. 23 (letter requesting redactions of declarant and certain other identifying information). Google seeks to prevent similar actions here.

Courts may redact the name of a declarant when publishing the individual's name "may increase the likelihood of future threatening behavior, implicating concerns of witness safety and the danger of impairing judicial efficiency." *E.g.*, *SEC v. Ripple Labs, Inc.*, 2023 WL 3477552, at *2 (S.D.N.Y. May 16, 2023) (redacting "the names and other identifying information of its expert witnesses and investor declarants"). Google's proposed redactions are justified under those precedents, and "are 'necessary to preserve higher values' of witness safety and judicial efficiency." *Id.* (quoting *Lugosch v. Pyramid Co. of Onondaga*, 435 F.3d 110, 124 (2d Cir. 2006)).

Conversely, the requested redactions have only a small impact on the public's right of access. The redactions Google seeks—to only a few isolated mentions of the declarants' names and other identifying information—are "narrowly tailored to protect only this sensitive ... information." *Kewazinga Corp. v. Microsoft Corp.*, 2021 WL 1222122, at *6 (S.D.N.Y. Mar. 31, 2021). They offer meaningful protection to the declarants' privacy interests but do not unduly infringe on the Court's interest in public access to information.

Second, the Court should redact the portions of the Google and NAXO Declarations detailing aspects of those firms' investigative processes, including their identification of a specific phishing domain, the email addresses associated with that domain, digital fingerprints associated with Defendants' software, and Google's explanation of those findings. Specifically, Google requests that the Court redact: the email addresses in paragraphs 32, 34, 35, and 36 of the Google Declaration; portions of the second sentence in paragraph 36 of the Google Declaration; portions of the second, third, fourth, and fifth sentences in paragraph 38 of the Google Declaration; and portions of paragraphs 65, 66, 67, 68, 69, 85, 92, 93, 103, 104, 105, 107, and 113 of the NAXO Declaration. *See* Google Decl. ¶¶ 32, 34–36, 38; NAXO Decl. ¶¶ 65–69, 85, 92–93, 103–105, 107, 113. Disclosure of this information reveals specific investigative methods, which may cause

cybercriminals to change their behavior, and can adversely impact other—and future—investigations.

Courts protect information about investigations from public disclosure that "could alert the targets of the investigation and could lead to efforts by them to frustrate the ongoing investigations." *United States v. Smith*, 985 F. Supp. 2d 506, 535 (S.D.N.Y. 2013) (issuing a protective order to prevent disclosure of discovery materials related to ongoing investigations); *see also, e.g.*, *Marigrove, Inc. v. Sauer de Arruda Pinto*, 2015 WL 13857424, at *8 (S.D. Fla. Mar. 30, 2015) (explaining that "one of the reasons for … sealing" documents "was to conduct the investigation in a way that would not tip off its targets"); *Matter of Search of Office Suites for World & Islam Stud. Enter.*, 925 F. Supp. 738, 740 (M.D. Fla. 1996) (sealing papers where "revelation of these matters would likely frustrate the ongoing investigation"); *cf. Adtrader, Inc. v. Google LLC*, 2020 WL 6395513, at *2 (N.D. Cal. Feb. 4, 2020) (sealing information about "systems functionality related to detecting and addressing invalid activity and processing associated advertising payments" which "individuals could use to manipulate Google's systems information about how Google detects and reacts to invalid activity"); *In re Google Inc. Gmail Litig.*, 2013 WL 5366963, at *3 (N.D. Cal. Sept. 25, 2013) (sealing information about "how users' interactions with the Gmail system affects how messages are transmitted" because "hackers and spammers could use this information to circumvent Google's anti-virus and anti-spam mechanisms").

Those concerns are implicated here. To aid this Court's understanding of how Google and NAXO identified the domains in use by the criminal enterprise, those firms have disclosed both specific findings and specific investigative methods. Google Decl. ¶¶ 32, 34–36, 38; NAXO Decl. ¶¶ 65–69, 85, 92–93, 103–105, 107, 113. The identified domain, email addresses, and fingerprints

could alert Defendants to Google's disruption efforts before they have succeeded. Disclosure of these investigative approaches more generally could educate cybercriminals worldwide about Google's and NAXO's investigative capabilities and techniques, potentially enabling them to evade detection. Importantly, this case is not a one-off. Google employs these investigation methods—and similar methods—on an ongoing basis to identify and disrupt phishing activity and protect its users from cybercrime.

Further, Google's request to redact references to investigative methods is "narrowly tailored to protect only this sensitive … information" without unduly restricting public access. *Kewazinga Corp.*, 2021 WL 1222122, at *6.

Third, good cause exists for sealing Defendants' malicious domains listed in Appendices A and C and redacting any references to those domains in other documents. This relief is necessary to preserve Google's ability to seek effective injunctive relief and prevent Defendants from causing further harm. Appendices A and C list the specific internet domains where Defendants' malicious sites are currently located. "[T]he weight of the presumption of public access is balanced against competing interests, which include but are not limited to the danger of impairing law enforcement or judicial efficiency." *Kahle*, 2024 WL 5168057, at *2 (internal quotations omitted). Such competing interests are present here, because publishing the domains targeted for judicial relief would enable Defendants to obscure or relocate their infrastructure.

Defendants are a group of foreign cybercriminals who engage in relentless and persistent phishing attacks to steal personal and financial information. To commit these attacks, Defendants developed a software known as "Outsider"—essentially a phishing kit for dummies—that includes the necessary tools and instructions. Using Outsider and the Enterprise's resources, Defendants deceive victims into turning over accounts, passwords, banking information, and other sensitive

financial data. Defendants then use this information to steal victims' money or sell the information to other criminal actors.

Google seeks to disrupt the infrastructure Defendants use to commit their crimes, including the domains listed in Appendices A and C and referenced in Google's pleadings and supporting materials. To do so, Google must act quickly and without notice to Defendants of Google's intended targets to ensure that Defendants do not have an opportunity to change or move their infrastructure. Defendants are sophisticated, well organized, and have the means to evade disruption. If they receive notice of the domains Google seeks to disrupt, they could simply adjust their operations to carry out their schemes using new domains, as they have before.

Federal district courts routinely grant motions to seal and redact references to web infrastructure when a plaintiff seeks to disrupt malicious cyber threats engaging in fraudulent activities.[1] Good cause exists to seal Appendices A and C because public disclosure of the domains Google seeks to disrupt before Google has effectuated the disruption would allow Defendants to alter their operations to avoid disruption and thereby continue to profit from their unlawful activities at the expense of Google, Google's customers and users, and the general public.

* * * * *

[1] *See, e.g.*, *Google LLC v. Yucheng Chang and Does 1–25*, No. 25-cv-10440 (S.D.N.Y. Dec. 17, 2025), Dkt. 19 (sealing and redacting similar materials, including appendix listing domain targets and identifying information for declarants); *Google LLC v. Does 1–25*, No. 25-cv-04503 (S.D.N.Y. May 30, 2025), Dkts. 1, 22 (sealing similar filings, including appendix listing domain targets, to disrupt the "BadBox 2.0" botnet); *Google LLC v. Does 1–25*, No. 25-cv-09421 (S.D.N.Y. Nov. 25, 2025), Dkt. 25 (redacting identifying information of declarants); *Microsoft Corp. v. Duong Dinh Tu*, No. 23-cv-10685 (S.D.N.Y. Dec. 6, 2023), Dkts. 1, 10 (sealing similar filings to disrupt "Storm-1152" scheme in which Defendants used internet bots to open and sell fraudulent email accounts for criminal purposes); *Microsoft Corp. v. Nady and Does 1–3*, No. 24-cv-02013 (E.D. Va. Nov. 13, 2024), Dkt. 19 (sealing similar filings to disrupt the "ONNX" phishing scheme).

For these reasons, Google requests that the Court grant Google's motion, allowing (1) the declarants' names and other identifying information to be redacted, (2) portions of the Google and NAXO Declarations detailing investigative processes and findings to be redacted, and (3) Appendices A and C be sealed and references to its contents to be redacted.

Dated: June 12, 2026

Respectfully submitted,

/s/ *Laura Harris*
Laura Harris
KING & SPALDING LLP
1290 Avenue of the Americas, 14th Fl.
New York, NY 10104-0101
Tel: (212) 556-2100
Fax: (212) 556-2222
lharris@kslaw.com

Benjamin S. Softness
KING & SPALDING LLP
50 California Street, Suite 3300
San Francisco, CA 94111-4624
Tel: (415) 318-1251
Fax: (415) 318-1300
bsoftness@kslaw.com

Counsel for Plaintiff Google LLC

CERTIFICATE OF COMPLIANCE

I, Laura Harris, an attorney duly admitted to practice before this Court, hereby certify pursuant to Local Rule 7.1(c), that the foregoing Plaintiff's Memorandum of Law in Support of Its Motion to File Appendices A and C Under Seal and Redact Certain Investigative and Identifying Information was prepared using Microsoft Word and contains 1,851 words in accordance with Local Rule 7.1(c).

Dated: June 12, 2026

/s/ *Laura Harris*
Laura Harris