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 FOR AN *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Other Authorities

INTRODUCTION

Google seeks an emergency *ex parte* temporary restraining order 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. Using powerful software designed to facilitate large-scale "phishing" attacks,[1] Defendants lure unsuspecting victims into entering their credit card information and other credentials on fraudulent websites designed to mimic the websites of legitimate organizations, including wireless telephone service providers, brokerage firms, toll-collection agencies, and even the United States Postal Service. The fraudulent websites often feature Google logos to enhance the illusion of legitimacy.

The software behind these attacks—called Outsider—is built and maintained by members of a criminal enterprise (the "Outsider Enterprise" or "Enterprise") who coordinate to identify targets, "phish" using deceptive text messages and ads, steal victims' personal and financial information, and monetize that stolen information. And the software makes this easy by removing the technical barriers that once constrained large-scale fraud: with Outsider, Enterprise members can create convincing-looking websites with a few clicks, no coding required. The Enterprise also exploits artificial intelligence ("AI") to supercharge these capabilities. It instructs its members how to use AI tools (like Google's Gemini technology) to generate *custom* website templates, which Outsider can then transform into phishing websites. The Enterprise's use of AI is part of a broader but disturbing pattern—by late 2025, phishing attacks generated using AI increased more than fourteenfold and accounted for over half of all reported phishing incidents.[2]

---

[1] "Phishing" is a cyberattack that tricks victims into clicking malicious links, often by sending false messages impersonating trusted brands.

[2] Alessandro Mascellino, *AI-Generated Phishing Surges As Attackers Shift Tactics, Hoxhunt Finds*, Expert Insights (Mar. 12, 2026), https://tinyurl.com/skhe5pwc.

The Outsider Enterprise has already stolen personal and financial information from victims across the globe, including in New York. Between May 18 and June 1, 2026, Google received more than 55,000 reports regarding fraudulent messages containing known Outsider phishing domains. And Google has already identified more than 1.59 million fraudulent sites. This number is not static. Google and other companies are working to thwart phishing attacks, while the Enterprise launches thousands of new sites every day. As long as the Enterprise's infrastructure remains operational, it will continue to defraud victims absent intervention.

The requested relief will disrupt the Enterprise's ongoing criminal activity by authorizing Google to disable the domains and servers the Enterprise uses to create its fraudulent sites, thereby disabling the Enterprise from reaching additional victims.

Google's application establishes the factors necessary to obtain a TRO and a preliminary injunction. *See Daileader v. Certain Underwriters at Lloyds London Syndicate 1861*, 96 F.4th 351, 356 (2d Cir. 2024). Courts in this District have granted injunctive relief in similar circumstances.[3] *First*, these schemes irreparably harm Google by damaging its brand and diverting its security resources. *Second*, Google is highly likely to prevail on the merits. Defendants are members of a criminal enterprise that conducts phishing attacks to defraud unsuspecting targets in the United States. They abuse Google products (such as Google Messages and Gemini) and Google's trademarks (the "Marks"). The Enterprise's criminal activities therefore violate the Racketeer

[3] *See, e.g.*, *Google LLC v. Doe 1 and Does 2-25 ("Google Darcula")*, No. 25-cv-10440 (S.D.N.Y. Dec. 17, 2025), Dkt. 18 (granting TRO to disrupt Darcula phishing software); *Google LLC v. Does 1-25 ("Google Lighthouse")*, No. 25-cv-09421 (S.D.N.Y. Nov. 12, 2025), Dkt. 18 (granting TRO to disrupt Lighthouse phishing software); *Google LLC v. Does 1-25*, No. 25-cv-04503 (S.D.N.Y. July 1, 2025), Dkt. 18; *Microsoft Corp. v. Does 1-2*, 2022 WL 18359421, at *4 (E.D. Va. Dec. 27, 2022), *R&R adopted*, 2023 WL 289701 (E.D. Va. Jan. 18, 2023); *Google LLC v. Starovikov*, 2021 WL 6754263, at *1 (S.D.N.Y. Dec. 16, 2021); *CME Grp. Inc. v. Nagovskiy*, 2019 WL 13252902, at *2 (N.D. Ill. Mar. 7, 2019).

Influenced and Corrupt Organizations Act ("RICO") and the Lanham Act. *Third* and *fourth*, the equities and the public interest entirely support Google.

To prevent irreparable harm, relief must be *ex parte*. Advance notice could frustrate the very relief Google seeks by allowing Defendants the opportunity to move their malicious infrastructure and conceal evidence of their misconduct. If this Court grants the emergency relief requested, Google will provide Defendants with notice after executing the disruption (and before a preliminary injunction hearing) through service as detailed below.

BACKGROUND

Defendants Does 1-25 are cybercriminals, co-conspirators, and members of the Outsider Enterprise. They operate a phishing ring using a software suite known as "Outsider." Compl. ¶¶ 1, 16-18; Declaration of [redacted] ("Google Decl.") ¶¶ 3-4, 26-27; Declaration of [redacted] ("NAXO Decl.") ¶¶ 6, 18-21. Members of the Enterprise license the software, use it to advance their schemes, and coordinate using dedicated Telegram channels. Compl. ¶¶ 1-4, 58, 64, 78-79; NAXO Decl. ¶¶ 22, 123-45. They have caused significant harm to Google and the public. Compl. ¶¶ 141-60; Google Decl. ¶¶ 56-63.

A. The Outsider Software

"Phishing" is a form of cybercrime that tricks targets into revealing sensitive information (such as banking or credit card information) through deceptive emails, text messages, or websites. Compl. ¶ 25; Google Decl. ¶¶ 22-23. A typical phishing message might alert the victim to an unpaid toll and provide a link to a site on which the victim can satisfy the debt. Compl. ¶¶ 122-28; NAXO Decl. ¶¶ 8-10. In fact, there is no toll, and the link leads to a fraudulent website, created by the scammer; any information the victim enters is stolen and used to enrich the scammer. Compl. ¶¶ 127-28; NAXO Decl. ¶¶ 35-36. These schemes have been enormously profitable, as has

licensing the infrastructure necessary to execute them—a business model known as Phishing-as-a-Service ("PhaaS"). Compl. ¶¶ 30-31; Google Decl. ¶¶ 22-25.

The Outsider software makes creating these fraudulent websites quick and easy; it also tracks the information victims enter on the sites and helps store the stolen information online. Compl. ¶¶ 34-35, 47-48, 56; Google Decl. ¶¶ 26-27. It is essentially a "phishing for dummies" kit that replaces coding and technical expertise with a plug-and-play interface. Compl. ¶ 1; NAXO Decl. ¶¶ 19, 21, 25.

Creating a site. Using Outsider, Enterprise members create phishing websites two different ways: (1) the user can select from more than 290 premade templates the software provides, Compl. ¶¶ 36-37; NAXO Decl. ¶¶ 76-80; or (2) the user can design a custom website template that Outsider can then convert into a phishing site that steals from consumers. Compl. ¶¶ 40-43; NAXO Decl. ¶¶ 56-61. Although the custom approach would ordinarily require technical expertise, Outsider provides Enterprise members step-by-step instructions for using generative AI tools, including Google's Gemini, to code custom shell websites. Compl. ¶ 41; NAXO Decl. ¶ 56. Enterprise members can then copy the AI-generated code into Outsider's "custom template" editor, which turns the template into a fraudulent website. Compl. ¶ 43; NAXO Decl. ¶ 57-59. The software is so powerful that the Outsider websites are nearly indistinguishable from the legitimate websites they mimic. *Id.* ¶ 124; NAXO Decl. ¶ 9, 84-85. In particular, the Enterprise's fake websites often include trademarked Google logos (such as the YouTube logo, which on a legitimate site provides a link to the site owner's YouTube channel) to lend the websites a veneer of legitimacy. Compl. ¶¶ 145-49; Google Decl. ¶¶ 50-51.

Tracking activity. Once the fraudulent website is live, Outsider tracks visitors to the site and the information they enter. Compl. ¶¶ 47-48; NAXO Decl. ¶¶ 85-87. As information is typed

into the fields on the site, Outsider tracks the victims' keystrokes in real time; in particular, credit card numbers are automatically formatted on the Outsider dashboard to resemble a physical credit card. Compl. ¶¶ 47-49; NAXO Decl. ¶¶ 85-87. The image of the "card" can then be scanned into a digital wallet and used to steal funds from the victims. Compl. ¶¶ 48-49; NAXO Decl. ¶¶ 85-87.

Cloud storage. Outsider provides a centralized platform for managing the infrastructure necessary to host a site and store stolen data. Compl. ¶ 56; NAXO Decl. ¶¶ 90-93. For example, Enterprise members can request assistance purchasing Google Cloud infrastructure to host their sites. Compl. ¶¶ 82, 154; NAXO Decl. ¶¶ 92-99. Outsider also included an integration with Google Drive that allowed users to export stolen data to Google's cloud-based document storage. Compl. ¶ 56; NAXO Decl. ¶¶ 90-92. Google blocked this functionality. Compl. ¶ 57; Google Decl. ¶ 45.

B. The Outsider Enterprise

The identities of the individuals who constitute the Outsider Enterprise are unknown. Compl. ¶¶ 17-18; Google Decl. ¶¶ 29, 37. But Google, NAXO, and other investigators have identified at least five interconnected threat groups that collectively manage and participate in the Enterprise. Compl. ¶¶ 58-96; NAXO Decl. ¶¶ 116-45. These threat groups develop, distribute, and deploy the Outsider software to carry out the Enterprise's phishing schemes, and they depend on each other's specialized contributions to execute those schemes—some of the members may even play multiple roles. Compl. ¶¶ 58, 95-96; NAXO Decl. ¶¶ 123-45.

- The **Developer Group** designs, maintains, and updates the Outsider software. Compl. ¶¶ 59-63; NAXO Decl. ¶¶ 22-27.
- The **Telegram Group** connects members of the Enterprise by managing the online communities through messaging channels on the encrypted Telegram app, where members distribute Outsider and coordinate specific phishing schemes. Compl. ¶¶ 78-93; NAXO Decl. ¶¶ 119-20, 143-44.
- The **Data Broker Group** acquires and supplies mass lists of potential victims' contact information. Compl. ¶¶ 65-68; NAXO Decl. ¶¶ 124-25.

- The **Spammer Group** handles the text messaging: once contact information is acquired, messaging victims *en masse* to lure them to the fake sites can require numerous automated cell phone banks coordinated by Enterprise members with the relevant resources and know-how. Compl. ¶¶ 69-72; NAXO Decl. ¶¶ 127-31.

- And the **Theft Group** monetizes the stolen information and credentials: for example, they load virtual copies of stolen credit cards into digital wallets like Google Wallet and route payments back to the Enterprise through tap-to-pay terminals or they sell stolen information to other criminals for further illicit use. Compl. ¶¶ 73-77; NAXO Decl. ¶¶ 132-35.

Acting together, the threat actor groups develop, execute, and profit from the Enterprise's numerous criminal phishing schemes. Compl. ¶¶ 58, 96; NAXO Decl. ¶¶ 19-21.

C. The Outsider Enterprise's Criminal Schemes

The Enterprise uses Outsider to carry out a wide range of coordinated criminal phishing schemes. As public awareness has grown of scams involving unpaid tolls or undelivered packages, the Enterprise has adapted its tactics, impersonating new categories of trusted institutions—such as wireless carriers or brokerage firms—to lure potential victims to enter personal and financial information into fraudulent websites. Compl. ¶¶ 99, 101; NAXO Decl. ¶¶ 28-32, 37-44. We detail here examples of known Outsider schemes.

The Telecommunications Scheme. In this scheme, the Enterprise impersonates major wireless carriers offering "rewards" that can be redeemed on their websites. Compl. ¶ 103; NAXO Decl. ¶¶ 37-44. Victims receive text messages, purportedly from their mobile provider, informing them that they have accumulated points or rewards redeemable for free products at a website linked in the text. Compl. ¶ 103; NAXO Decl. ¶¶ 37-42. The linked page encourages victims to select a product that they have earned with their "rewards"—often with high-value products such as name brand headphones or watches as lure—and tells them all that is needed to complete the transaction is payment of a small shipping fee. Compl. ¶¶ 104-07; NAXO Decl. ¶¶ 42-43. Of course, the site

is fake—there are no rewards or products—and as victims enter their payment information, Outsider tracks their keystrokes and steals the information. Compl. ¶ 108; NAXO Decl. ¶ 44.[4]

The Brokerage Firm Scheme. In this scheme, the Enterprise sends phishing texts to targets impersonating brokerage firms or other financial institutions, falsely warning recipients that their account has been restricted. Compl. ¶¶ 110-11; NAXO Decl. ¶¶ 28-29. The texts direct targets to a page mimicking the financial institution's website. Compl. ¶ 112; NAXO Decl. ¶¶ 29-30. When the victims enter their login credentials on the fake site, the Enterprise (through its keystroke logging) acquires the victims' login information which it can then use at the real institution or sell. Compl. ¶¶ 113-14; NAXO Decl. ¶¶ 31-32, 85-86.

Once the Enterprise has access to a victim's brokerage account, it can liquidate assets, steal funds, or leverage the account for market manipulation. Compl. ¶¶ 116-17; NAXO Decl. ¶¶ 20-21. One increasingly common tactic is a modern version of "pump and dump." Compl. ¶ 117; NAXO Decl. ¶ 21. After acquiring shares of a specific stock in their own accounts, Enterprise members use victims' accounts to make subsequent purchases of the same security—to "pump" the stock price—before selling ("dumping") their own shares at the artificially inflated price. Compl. ¶ 117; NAXO Decl. ¶ 21.

The Delivery Scheme. In this scam, the Enterprise sends a text message—purportedly from the USPS, for example—telling targets that they have an undelivered package. Compl. ¶ 120; NAXO Decl. ¶ 33. To "complete delivery," the victim must pay a small delivery fee by clicking the link provided, which directs them to a phishing site. Compl. ¶ 121; NAXO Decl. ¶ 33. Once

[4] Because Outsider tracks keystrokes in *real time*, one need not even click a purported "Submit" or "Pay" button on the fraudulent site in order to be victimized; it is enough to type the number. *See* Compl. ¶ 108; NAXO Decl. ¶¶ 85-86.

on the website, targets are prompted to enter their personal and financial information, all of which Outsider captures in real time. Compl. ¶ 121; NAXO Decl. ¶¶ 33, 85-86.

The Toll Scheme. The Enterprise's Toll Scheme works much the same way: the text states that the target has a past-due toll violation and links to a page—which might mimic, for example, New York's E-Z Pass toll agency website—where the target can pay the purported toll. Compl. ¶¶ 122-28; NAXO Decl. ¶¶ 34-36. When the victims enter their personal financial information, it is logged and stolen. Compl. ¶¶ 127-28; NAXO Decl. ¶ 35.

The E-Commerce Scheme. In this phishing scheme, the Enterprise uses Outsider to create fraudulent e-commerce websites mimicking legitimate online retailers. Compl. ¶¶ 129-30; NAXO Decl. ¶¶ 46-55. Victims are directed to these sites through search results or online advertisements for real products that the Enterprise places on legitimate platforms—only the ads link to the Enterprise's fake storefronts. Compl. ¶¶ 130-34; NAXO Decl. ¶¶ 48-50. The Enterprise then deploys those ads on social media or other web sites. Compl. ¶ 133; NAXO Decl. ¶¶ 49-50. The ads direct victims to fake sites that peddle familiar products and prompt victims, at checkout, to enter payment and shipping information. Compl. ¶¶ 133-36; NAXO Decl. ¶¶ 50-51. To enhance their credibility, the websites often display logos associated with well-known electronic payment services, such as Google Pay. Compl. ¶¶ 136-37; NAXO Decl. ¶¶ 50-51. Of course, the products never arrive, the payment pages are fake, and the information entered by the victim is stolen. Compl. ¶¶ 133, 138-40; NAXO Decl. ¶ 49.

D. The Outsider Enterprise Harms Google and the Public

The Outsider Enterprise steals victims' money and sensitive personal information. Compl. ¶¶ 141-42; Google Decl. ¶¶ 56-57. It also harms Google and other businesses it mimics by eroding customer trust and goodwill. Compl. ¶¶ 143, 150; Google Decl. ¶¶ 57-59, 62. Specifically, the

Enterprise has created fraudulent websites featuring Google's branding or logos (e.g., YouTube, Google Play, and Google Pay). Compl. ¶ 145; Google Decl. ¶¶ 50-53. As an institutional technology brand, victims may interpret the presence of these Google logos as an indicator that the website is safe and authentic. Compl. ¶ 149; Google Decl. ¶ 55. The Outsider Enterprise thus exploits Google branding—and the goodwill associated with it—to convince victims to disclose sensitive information. Compl. ¶ 149; Google Decl. ¶ 55. The Enterprise also misuses Google products like Gmail, Google Cloud and Gemini, violating various Google usage policies. Compl. ¶¶ 151-57; Google Decl. ¶¶ 39-49.

The Enterprise's crimes have also imposed significant financial costs on Google. Compl. ¶¶ 158-60; Google Decl. ¶¶ 57-61. To counter these schemes, Google devotes substantial financial and technical resources to investigating the Enterprise's activities, developing measures to detect and prevent phishing attacks on its platforms, and remediating the harms the Enterprise has caused. Compl. ¶¶ 158-60; Google Decl. ¶¶ 57-59.

The Enterprise's widespread phishing attacks across multiple industries demonstrate that it is a sophisticated group with significant reach. Compl. ¶ 97; NAXO Decl. ¶¶ 27, 146-47. Outsider removes the technical barriers that once constrained phishing operations, allowing the Enterprise to deploy attacks rapidly, replicate them with ease, and cause staggering harm. Compl. ¶¶ 5, 10, 34; NAXO Decl. ¶¶ 9, 19. Between May 18 and June 1, 2026, Google received more than 55,000 reports from users who received fraudulent messages containing links to Outsider Enterprise's phishing domains. Compl. ¶ 144; Google Decl. ¶ 42. Without disruption, the Enterprise will continue to conduct its phishing schemes, generate new streams of illicit revenue, and channel those proceeds into entrenching its operations and expanding to other criminal activities. Compl. ¶ 173; Google Decl. ¶ 67.

ARGUMENT

I. This Court Should Issue a TRO and Order to Show Cause for a Preliminary Injunction

A plaintiff is entitled to a TRO and preliminary injunction where (1) it "is likely to suffer irreparable harm in the absence of" relief; (2) it is "likely to succeed on the merits" (or at least raises "sufficiently serious questions"); (3) the "balance of equities tips in [its] favor"; and (4) "an injunction is in the public interest." *Citigroup Glob. Mkts., Inc. v. VCG Special Opportunities Master Fund Ltd.*, 598 F.3d 30, 34-35 (2d Cir. 2010). Courts balance the factors "like a sliding scale," such that "more of one excuses less of the other." *Thapa v. Gonzales*, 460 F.3d 323, 334 (2d Cir. 2006) (quotation marks and citation omitted); *Citigroup*, 598 F.3d at 35-38 & n.8 (emphasizing "[t]he value of this circuit's approach to assessing the merits of a claim at the preliminary injunction stage lies in its flexibility"). That said, "[i]rreparable harm is the single most important prerequisite." *Faiveley Transp. Malmo AB v. Wabtec Corp.*, 559 F.3d 110, 118 (2d Cir. 2009) (quotation marks and citation omitted). Furthermore, given the grave threat of irreparable harm, this Court may grant Google relief if it concludes that Google's claims raise "serious question[s] going to the merits to make them a fair ground for trial." *Citigroup*, 598 F.3d at 33 (cleaned up).

Here, every factor weighs in Google's favor. The Enterprise is causing ongoing and irreparable harm to Google and the public. It uses phishing attacks to defraud unsuspecting targets and steal personal and financial information while impairing Google's reputation and goodwill and causing Google (and numerous others) unrecoverable financial losses, in violation of at least two federal statutes. And the equities and public interest analyses decidedly favor Google: absent disruption, the Enterprise will continue to profit from its unlawful activities at the expense of Google and an ever-increasing number of victims. This is a quintessential case meriting emergency

relief. It is thus no surprise that courts have granted preliminary relief in similar cases involving unknown persons or entities operating ongoing harmful phishing schemes. *See, e.g.*, *Google Darcula*, Dkt. 18; *Google Lighthouse*, Dkt. 18; *Microsoft Corp.*, 2022 WL 18359421, at *4; *CME Grp. Inc.*, 2019 WL 13252902, at *2.

A. Google and the Public Will Suffer Irreparable Harm Absent Relief

The Enterprise defrauds more victims, steals more information and money, abuses Google's trademarks, and injures Google's goodwill and reputation every day. Compl. ¶¶ 141, 145, 146, 150; Google Decl. ¶¶ 59-62. It is well-established that a company's "loss of reputation, good will, and business opportunities" constitutes irreparable harm. *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 404 (2d Cir. 2004); *accord Church of Scientology Int'l v. Elmira Mission of the Church of Scientology*, 794 F.2d 38, 44 (2d Cir. 1986). Google has invested significant resources to develop strong brand recognition associated with its name, logos, and products. Compl. ¶¶ 185-86; Google Decl. ¶¶ 5-9. The harm to Google is compounded by the substantial financial resources Google has devoted (and continues to devote) to combat the Enterprise's phishing schemes. Compl. ¶ 158; Google Decl. ¶¶ 57-61.

The irreparable harm to Google is especially clear here given the doubt that it will ever be made whole—even after final judgment—because the Enterprise is composed of elusive cybercriminals unlikely to comply with any judgment. *See, e.g.*, *Brenntag Int'l Chemicals, Inc. v. Norddeutsche Landesbank GZ*, 9 F. Supp. 2d 331, 345 (S.D.N.Y. 1998) ("[W]here a plaintiff's injury is theoretically compensable in money damages but, as a practical matter, the defendant would not or could not respond fully for those damages, preliminary injunctive relief has been deemed necessary to protect the plaintiff from irreparable injury."), *aff'd sub nom.*, *Brenntag Int'l Chemicals, Inc. v. Bank of India*, 175 F.3d 245 (2d Cir. 1999). Moreover, Google is entitled to a presumption of irreparable harm upon showing, as it does here, a likelihood of success on its claims

under the Lanham Act. *See* 15 U.S.C. § 1116(a); *Two Hands IP LLC v. Two Hands Am., Inc.*, 563 F. Supp. 3d 290, 300 (S.D.N.Y. 2021).

B. Google Is Likely to Succeed on the Merits

Google need only show that it is "likely to succeed" or that there are sufficiently "serious questions going to the merits to make them a fair ground for litigation." *Citigroup*, 598 F.3d at 34-35 (cleaned up). In any event, Google is highly likely to succeed on each claim. It has supported its motion with declarations from an investigator in Google's CyberCrime Investigation Group and from NAXO, an investigations firm. Both declarations provide detailed evidence of Defendants' wrongdoing and the irreparable harm it has caused and will continue to cause. Given the strength of this evidence, the likelihood of success weighs heavily in favor of granting relief.

(i) Google's Lanham Act Claims Are Likely to Succeed

Defendants' unauthorized use of Google branding violates the Lanham Act's prohibitions on trademark and service mark infringement, as well as its related prohibitions on false endorsement and sponsorship, false designation of origin, false advertising, and unfair competition.

Section 1114 of the Lanham Act prohibits infringement of a registered trademark or service mark. Infringement occurs when any person, without the consent of the registrant, "use[s] in commerce any reproduction, counterfeit, copy, or colorable imitation of a registered mark in connection with the sale, offering for sale, distribution, or advertising of any goods or services" and "such use is likely to cause confusion, or to cause mistake, or to deceive." 15 U.S.C. § 1114(1)(a). A plaintiff need only show that (1) it has a valid, protectable mark and (2) defendants' use of that mark in commerce is likely to cause confusion among consumers. *See Virgin Enters. Ltd. v. Nawab*, 335 F.3d 141, 146 (2d Cir. 2003). "In trademark cases, a showing of likelihood of confusion as to source or sponsorship establishes the requisite likelihood of

success on the merits as well as risk of irreparable harm .... To meet this burden, [the plaintiff] need[s] only to raise a serious question of likelihood of confusion." *Am. Cyanamid Co. v. Campagna Per Le Farmacie in Italia, S.P.A.*, 847 F.2d 53, 55 (2d Cir. 1988) (cleaned up).

Defendants' liability under these provisions is straightforward. Google has valid, protectable rights to the Marks with relevant, often incontestable, registrations. *See* App'x D, Google Decl. ¶¶ 50-53 (detailing Google's registrations for the relevant Marks). And Defendants misappropriate those Marks to deceive the public, which is likely to cause confusion and mistake. *See, e.g.*, *CME Grp. Inc.*, 2019 WL 13252902, at *1-2 (finding a "likelihood of confusion" where defendants perpetrated a phishing scheme using plaintiff's marks). Indeed, in this case confusion is the point: Defendants exploit Google's trustworthy and well-known Marks on their phishing sites to cause their targets to reveal information *that they believe they are revealing to someone else*. Such schemes are paradigmatic Lanham Act violations. *See, e.g.*, *id.* (finding Lanham Act liability where defendants used plaintiff's marks "in connection with a phishing scheme designed to solicit or request personally identifiable information, such as user IDs and passwords, from consumers"); *Sapient Corp. v. Okorie*, 2019 WL 1983230, at *2 (N.D. Cal. Mar. 26, 2019) (similar).[5]

Additionally, section 1125(a) prohibits "false designation[s] of origin" that are likely to cause confusion as to the "origin, sponsorship, or approval" of a product or service. 15 U.S.C. § 1125(a)(1)(A). A claim under section 1125(a)(1)(A) has the same elements as a claim under section 1114(1) and can be established with the same evidence, *see Victorinox AG v. B&F Sys.,*

[5] *See also, e.g.*, *Yahoo! Inc. v. XYZ Cos.*, 872 F. Supp. 2d 300, 304 (S.D.N.Y. 2011) (upholding trademark infringement claim where defendants intentionally copied plaintiff's name and marks in emails designed to mislead victims into thinking they won lotteries affiliated with plaintiff).

Inc., 114 F. Supp. 3d 132, 139 (S.D.N.Y. 2015). Google's section 1125(a)(1)(A) claim is thus likely to succeed for the same reasons.

Section 1125(a) also prohibits false advertising. 15 U.S.C. § 1125(a)(1)(B). To qualify as false advertising, a representation must be (1) false, (2) material, (3) placed in interstate commerce, and (4) the cause of injury to the plaintiff. *Church & Dwight Co. v. SPD Swiss Precision Diagnostics, GmBH*, 843 F.3d 48, 65 (2d Cir. 2016). Falsity requires a showing that a challenged advertisement is false on its face or that the advertisement, "while not literally false, is nevertheless likely to mislead or confuse consumers." *Apotex Inc. v. Acorda Therapeutics, Inc.*, 823 F.3d 51, 63 (2d Cir. 2016) (cleaned up). For materiality, a plaintiff "must also demonstrate that the false or misleading representation involved an inherent or material quality of the product." *Id.* (quoting *Time Warner Cable, Inc. v. DirectTV, Inc.*, 497 F.3d 144, 153 n.3 (2d Cir. 2007)). "When an advertisement is false on its face or false by necessary implication, a court may grant relief 'without reference to the advertisement's actual impact on the buying public' because consumer confusion is presumed." *Playtex Prods., LLC v. Munchkin, Inc.*, 2016 WL 1276450, at *4 (S.D.N.Y. Mar. 29, 2016) (quoting *Time Warner*, 497 F.3d at 153).

Here, Defendants deceive internet users by featuring Google's Marks on their fraudulent websites, falsely marketing their scam as bearing Google's approval or involvement. Compl. ¶ 149; Google Decl. ¶¶ 50-52, 55. That fraudulent marketing scheme easily satisfies the elements of false advertising. The representations are literally false because the websites are not from or endorsed by Google, and the unauthorized use of the Google Marks in connection with the fraudulent schemes violates Google's terms of service. *See* Compl. ¶¶ 148-54; Google Decl. ¶¶ 53-55. The representations are material because they are critical to the success of the phishing operation. Defendants' schemes succeed *because* their websites appear to be real—they rely on

consumer trust in the Google Pay, Google Play, and YouTube Marks. *See* Compl. ¶ 149; Google Decl. ¶ 50.

The messages using Google's Marks are also placed in interstate commerce via the internet. *See* Compl. ¶ 98; Google Decl. ¶¶ 40-41. The messages cause injury to Google by damaging its hard-earned goodwill, tarnishing its Marks by association with fraud, and forcing it to spend substantial resources to combat these scams and protect its intellectual property. *See* Compl. ¶¶ 143, 158-60; Google Decl. ¶¶ 57-61. Defendants thus violated the Lanham Act in multiple ways, many times over. For all these reasons, and as prior cases have held on similar facts, Google's Lanham Act claims are likely to succeed on the merits. *See, e.g.*, *Google Darcula*, Dkt. 18, at 4-5 (Google likely to succeed on Lanham Act claims where members of cybercriminal enterprise "exploit[ed] Google's trustworthy, well-known, valid, protectable, and registered Marks on their spoofed websites to deceive consumers"); *Google Lighthouse*, Dkt. 18, at 4-5 (same).

(ii) Google's RICO Claim Is Likely to Succeed

Google is likely to prevail on its RICO claim. *See, e.g.*, *Google Darcula*, Dkt. 18, at 5-6 (Google likely to succeed on RICO claims where defendants use "software to dupe people in the United States and around the world into clicking on malicious links leading to spoofed websites as part of phishing schemes"); *Google Lighthouse*, Dkt. 18, at 5-6 (same). To prove a RICO claim, a plaintiff must establish that the defendant engaged in "(1) conduct (2) of an enterprise (3) through a pattern (4) of racketeering activity." *DeFalco v. Bernas*, 244 F.3d 286, 306 (2d Cir. 2001) (cleaned up). The defendant also must have engaged in "interstate or foreign commerce" in carrying out these acts. *See Hinterberger v. Catholic Health Sys., Inc.*, 536 F. App'x 14, 16 (2d Cir. 2013). And the defendant must have caused "an injury to business or property." *DeFalco*, 244 F.3d at 305. A private plaintiff is entitled to equitable relief when it demonstrates injury under

RICO. *See State Farm Mut. Auto. Ins. Co. v. Tri-Borough NY Med. Prac. P.C.*, 120 F.4th 59, 95 (2d Cir. 2024).

Google satisfies each of the required elements of a RICO claim. The Outsider Enterprise is a digital incarnation of organized crime, and it carries out its illicit activities not only in New York but across the United States and around the world. Defendants share a common purpose of defrauding victims into disclosing sensitive personal information, including financial account details, and stealing their money. United by the Outsider software and the online community that enables its use, the Enterprise quickly and easily coordinates sophisticated phishing schemes. Those schemes tarnish Google's reputation, hurt Google's customers, and require Google to incur costs investigating the Enterprise's racketeering activity, injuring Google's business or property as a direct result of the Enterprise's operations.

1. Conduct. To satisfy the conduct element, a plaintiff must establish that the defendants had "some part in directing [the enterprise's] affairs." *DeFalco*, 244 F.3d at 309 (cleaned up). This standard is "not limited to those with primary responsibility," nor is it limited to those "with a formal position in the enterprise." *Id.* (cleaned up). Here, each Defendant had at least "some part" in the Outsider Enterprise. *See id.*; *see also* Compl. ¶¶ 58-96; NAXO Decl. ¶ 19. Members of the Enterprise each take part in directing aspects of its activities: some develop the PhaaS software, architecture, and user interface; others create and manage an online community that recruits other Enterprise members and facilitates communication and coordination; others supply potential victims' contact information; others specialize in bulk SMS messaging; and yet others steal more of a victim's information and money after the Enterprise acquires phished credentials. Compl. ¶¶ 58-96; NAXO Decl. ¶ 19. The Enterprise works together to implement its schemes; none of the

schemes can generate revenue without the Enterprise members' cooperation. *See* Compl. ¶ 58; NAXO Decl. ¶ 19.

2. Enterprise. To show that the defendants participated in and operated as an enterprise, a plaintiff must establish (1) "a common purpose of engaging in a course of conduct"; (2) "an ongoing organization, formal or informal"; and (3) "evidence that the various associates function as a continuing unit." *DeFalco*, 244 F.3d at 307 (quoting *United States v. Turkette*, 452 U.S. 576, 583 (1981)). The Enterprise members' common purpose is clear: to enrich themselves by executing a wide variety of coordinated phishing schemes. Compl. ¶ 168; NAXO Decl. ¶¶ 19, 123-36.

Defendants play interdependent roles, with the Enterprise relying "on the actions of each of the Defendants to execute its fraudulent scheme." *1567 56th St., LLC v. Spitzer*, 774 F. Supp. 3d 476, 490 (E.D.N.Y. 2025). For example, Defendants can use Outsider (built and maintained by the Developer Group) to build phishing websites either based on one of over 290 templates or by using AI to create a custom site. Compl. ¶¶ 35-45; NAXO Decl. ¶¶ 45-48, 56-61. They can then turn to the Enterprise's Telegram channels (operated by the Telegram Group) to coordinate phishing activities across the Data Broker, Spammer, and Theft Groups. Compl. ¶¶ 58-93; NAXO Decl. ¶¶ 19, 123-36. Through the Outsider software and the accompanying online community, Defendants "pool[] their resources, knowledge, skills, and labor to achieve through th[at] enterprise efficiencies ... that none of them could have achieved individually." *Safe Streets All. v. Hickenlooper*, 859 F.3d 865, 883 (10th Cir. 2017). Defendants thus function as a unit. *See United States v. Errico*, 635 F.2d 152, 156 (2d Cir. 1980) (affirming finding of RICO enterprise where a "network of jockeys and bettors" "came together" to "profit from the illegal fixing of races"). Google has provided strong evidence establishing that Defendants are a group of persons

associated together, as a continuing unit, for the common purpose of carrying out criminal activities.

3. Pattern. To show a "pattern" of racketeering activity under RICO, a plaintiff must establish "at least two acts of racketeering activity, one of which occurred [after 1970] and the last of which occurred within ten years ... after the commission of a prior act of racketeering activity." *DeFalco*, 244 F.3d at 306 (quoting 18 U.S.C. § 1961(5)); 18 U.S.C. § 1961(1) (defining "racketeering activity" to include various state and federal crimes). The racketeering activity must exhibit "continuity" over time. *United States v. Aulicino*, 44 F.3d 1102, 1111 (2d Cir. 1995). Continuity is especially easy to demonstrate where the aims of the enterprise are "inherently unlawful." *Id*. Google's evidence clearly demonstrates that the Enterprise's criminal conduct constitutes a "pattern" within the meaning of the statute. Compl. ¶ 144; Google Decl. ¶¶ 42, 59-62. Indeed, the Enterprise has stolen credit card information from over 100,000 individuals through its fraudulent text messages directing those victims to its fraudulent websites. Compl. ¶ 141; NAXO Decl. ¶ 6. In the five-month period between November 14, 2025, to April 14, 2026, alone, Google detected more than 1.59 million webpages linked to the Outsider Enterprise. Compl. ¶ 141; Google Decl. ¶ 59. And there can be no doubt that the Enterprise's aims—to perpetrate phishing schemes—are inherently unlawful.

4. Racketeering. To show that a defendant engaged in racketeering activity, a plaintiff must establish that the defendant committed one or more of the predicate crimes enumerated in 18 U.S.C. § 1961(1). *See DeFalco*, 244 F.3d at 306. The predicate acts include violations of the federal wire fraud statute. 18 U.S.C. § 1343.

Wire fraud is the "transmitt[ing], by means of wire … communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing

[fraudulent] scheme[s].” 18 U.S.C. § 1343. The Enterprise commits wire fraud every time its members send text messages to trick individuals in the United States into unknowingly submitting sensitive personal or financial information through misrepresentation and deception in order to steal those victims’ money. *See Bascunan v. Elsaca*, 927 F.3d 108, 122 (2d Cir. 2019) (“There are three ‘essential elements’ to mail or wire fraud: ‘(1) a scheme to defraud, (2) money or property as the object of the scheme, and (3) use of the mails or wires to further the scheme.’” (citation and emphasis omitted)). Between May 18 and June 1, 2026, Google received more than 55,000 reports from users about fraudulent messages sent by the Outsider Enterprise to perpetrate phishing schemes to steal money from these targets. Compl. ¶ 144; Google Decl. ¶¶ 42-43. Defendants have committed wire fraud many times over and continue to do so today.

5. Injury. Defendants’ RICO violations have directly caused Google injury to its business and property. “A plaintiff has been ‘injured in his business or property’ if his business or property has been harmed or damaged. Section 1964(c) requires nothing more.” *Med. Marijuana, Inc. v. Horn*, 604 U.S. 593, 601 (2025). Moreover, the concept of injury under Section 1964(c) encompasses “damage of or to ... reputation.” *Id.* (cleaned up). The injury to Google’s business is an inherent component—and a direct result—of the Outsider Enterprise’s schemes. The Enterprise’s schemes dupe victims into disclosing sensitive information by mimicking trusted brands, government agencies, and financial institutions, and they include Google Marks in order to prey on the trust Google has earned from internet users. Moreover, Google must expend resources to respond to and remediate the business impact of the Outsider Enterprise’s schemes. It has been forced to spend hundreds of hours and significant financial resources investigating the schemes and pursuing other mitigation efforts, like suspending accounts. Compl. ¶ 160; Google

Decl. ¶¶ 58-61. Defendants' RICO violations have directly injured Google's business and property.

(iii) Google's RICO Conspiracy Claim Is Likely to Succeed

In addition to establishing a substantive RICO violation, Google can demonstrate that the Enterprise engaged in a RICO conspiracy. To establish that claim, Google need only prove that the Enterprise "conspire[d] to violate" the provisions of 18 U.S.C. § 1962(c). *Id.* § 1962(d). The overlapping links among the Defendants—including the "use of the [Outsider] software, communication over dedicated Telegram channels, and the methods used to deploy phishing schemes using [Outsider] and other Enterprise-controlled resources demonstrate that the Enterprise formed an agreement as part of a common scheme and conspiracy." *See Google Darcula*, Dkt. 18, at 6; *Google Lighthouse*, Dkt. 18, at 6; *see also* Compl. ¶¶ 58-96; NAXO Decl. ¶¶ 123-36. Because they agreed to form and operate the Enterprise and to commit the numerous predicate acts of fraud and related activity that make up the criminal activities, Defendants are liable under 18 U.S.C. § 1962(d).

C. The Balance of Equities Decidedly Favors a TRO

The Enterprise commits crimes, defrauds the public, and injures Google. "There is no legitimate reason why Defendants should be permitted to continue to weaponize Google's branding to defraud the public and commit cybercrimes." *Google Darcula*, Dkt. 18, at 7; *see also Google Lighthouse*, Dkt. 18, at 7; *Suber v. VVP Servs.*, 2021 WL 1101235, at *7 (S.D.N.Y. Mar. 23, 2021) (balance of hardships supported court's grant of *ex parte* injunctive relief where enterprise did not "have any right to use the profits of a fraudulent enterprise … to continue supporting their unlawful activities or for personal uses"); *FTC v. Verity Int'l, Ltd.*, 2000 WL 1805688, at *1 (S.D.N.Y. Dec. 8, 2000) (balance of equities weighs in favor of a TRO where an enterprise's practices likely violate a federal statute). It is "'axiomatic that an infringer ... cannot

complain about the loss of ability'" to continue infringing, *3M Co. v. CovCare, Inc.*, 537 F. Supp. 3d 385, 404 (E.D.N.Y. 2021) (quoting *WPIX, Inc. v. ivi, Inc.*, 691 F.3d 275, 287 (2d Cir. 2012)), and Defendants' misconduct poses "grave harm ... to [Google's] reputation and brand in the absence of an injunction." *Id.*[6]

D. The Public Interest Favors a TRO

Finally, a TRO would serve the public interest. The Outsider Enterprise has defrauded more than 100,000 victims, while using their ill-gotten funds to support further criminal schemes. *See* Compl. ¶¶ 33, 141, 144; NAXO Decl. ¶¶ 6, 20. With each day, Defendants deploy new phishing websites to deceive more victims. The public interest is served by enforcing statutes designed to protect the public—such as RICO and the Lanham Act—and by thwarting criminal activity with no legitimate justification whatsoever. *See, e.g.*, *Google Darcula*, Dkt. 18, at 7 (public interest is served by enforcing RICO and Lanham Act); *Google Lighthouse*, Dkt. 18, at 7 (same); *see also CME Grp. Inc.*, 2019 WL 13252902, at *3 (public interest is served by enforcing Lanham Act against phishing operation).

II. *Ex Parte* Relief Is Necessary Here

Rule 65 authorizes *ex parte* relief where immediate and irreparable injury will occur if the Court waits for notice and where there is good cause. *See* Fed. R. Civ. P. 65(b)(1). A TRO "may be ordered on an *ex parte* basis under subdivision (b) if the applicant makes a strong showing of the reasons why notice to the Defendants is likely to defeat effective relief." Fed. R. Civ. P. 65 committee notes to 2001 amendment; *accord In re Vuitton et Fils S.A.*, 606 F.2d 1, 5 (2d Cir. 1979) (per curiam). In other words, even where notice *could* be given, *ex parte* relief is appropriate where

[6] *See, e.g.*, *Microsoft Corp. v. Does 1-2*, 2024 WL 1708328, at *11 (E.D. Va. Jan. 10, 2024) ("Defendants would not suffer any hardship because an injunction would only require them to cease engaging in illegal activities."), *R&R adopted*, 2024 WL 1708323 (E.D. Va. Jan. 30, 2024); *Microsoft Corp.*, 2022 WL 18359421, at *5 (same with regard to similar phishing operation).

notice would "serve only to render fruitless further prosecution of the action." *In re Vuitton et Fils*, 606 F.2d at 5; *see also Granny Goose Foods, Inc. v. Bhd. of Teamsters*, 415 U.S. 423, 439 (1974).[7]

That is the situation here. The Enterprise is engaged in dynamic and technically sophisticated cybercrime; it is virtually certain "to delete or to relocate" its criminal internet infrastructure, "destr[oy] or conceal[] ... other discoverable evidence" of misconduct, and "warn … associates engaged in such activities" if given "advance notice of th[e] action." *E.g.*, *Sophos Ltd. v. Does 1-2*, 2020 WL 4722425, at *2 (E.D. Va. May 1, 2020); *see* Google Decl. ¶¶ 64-66; *accord Filipova v. Gezhong (7-21 Delivery)*, 2025 WL 2831148, at *3 (S.D.N.Y. Oct. 6, 2025) (granting *ex parte* relief where "Defendants may easily and quickly transfer or modify e-commerce store registration data and content, ... thereby thwarting Plaintiff's ability to obtain meaningful relief"); *Google LLC v. Starovikov, et al.*, No. 21-cv-10260 (S.D.N.Y. Dec. 7, 2021), Dkt. 8 (*Ex Parte* Temporary Restraining Order and Order to Show Cause Re: Preliminary Injunction).

Courts regularly grant *ex parte* relief in these circumstances. *See*, *e.g.*, *Google Darcula*, Dkt. 18 (granting *ex parte* TRO against similar phishing scheme); *Google Lighthouse*, Dkt. 18 (same); *Mirashi v. Doe*, 2025 WL 783353, at *5 (D.N.J. Mar. 12, 2025) (granting *ex parte* TRO against phishing scheme where "Plaintiff's attorney has certified that neither he nor Plaintiff knows the identi[t]y of the Hacker" and "alerting the Hacker … would likely prompt the Hacker to take more 'extreme measures' to 'conceal and dissipate the stolen Bitcoin'").

Moreover, to ensure that the *ex parte* relief is strictly limited to "serving [its] underlying purpose" and no more, *Granny Goose Foods Inc.*, 415 U.S. at 439, if the proposed order is granted,

[7] In any event, notice here is not possible because Google does not presently know Defendants' true identities.

Google will undertake efforts to locate and provide actual notice to Defendants of the TRO and preliminary injunction hearing, and will attempt to effect service of the relevant papers immediately upon effectuation of the injunctive relief in the proposed order, and in no event fewer than five days before the preliminary injunction hearing (or such time as the Court may order).

III. The Court Should Authorize Google to Serve Process by Alternative Means

Google also requests permission to serve Defendants by alternative means. Defendants are believed to reside in China, *see* Compl. ¶ 16; Harris Decl. ¶¶ 15-16, but Google does not know their precise identities or addresses. Federal Rule of Civil Procedure 4(f)(3) authorizes service by any court-ordered means "not prohibited by international agreement." Specifically, Google requests authorization to serve Defendants via (1) website publication 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.

Courts have long authorized alternative service through a variety of methods, "including publication, ordinary mail, … and most recently, email." *Rio Props., Inc. v. Rio Int'l Interlink*, 284 F.3d 1007, 1016 (9th Cir. 2002). Email and website publication are particularly appropriate where, as here, the addresses of foreign cybercriminal defendants are unknown. *See, e.g.*, *Microsoft Corp. v. Does*, 2012 WL 5497946, at *2 (E.D.N.Y. Nov. 13, 2012) (approving email service under Rule 4(f)(3) for "alleged cybercriminals whose personal identities and physical locations [were] unknown" where they "use[] sophisticated means to conceal their identities and locations"). In such cases, moreover, "combin[ing]" multiple means of alternative service reinforces its permissibility and effectiveness. *Juicero, Inc. v. Itaste Co.*, 2017 WL 3996196, at *3 (N.D. Cal. June 5, 2017); *Marvici v. Roche Facilities Maint. LLC*, 2021 WL 5323748, at *4 (S.D.N.Y. Oct. 6, 2021). Here, where Defendants have no ascertainable address and operate almost entirely online, service through website publication and email is most likely to be the most accurate and viable

means of notice and service. Other courts have repeatedly authorized service by website publication and/or email or electronic messaging in similar circumstances. *See*, *e.g.*, *Google Lighthouse*, Dkt. 18 (granting alternative service by website publication and email for foreign defendants involved in nearly identical phishing scheme).

Smart Study Co. v. Shenzhenshixindajixieyouxiangongsi, 164 F.4th 164 (2d Cir. 2025), does not preclude Google's requested approach. In *Smart Study*, the Second Circuit considered whether email service was appropriate under the Hague Convention. *See id.* at 170-73. But the Hague Convention does not apply here for two reasons. *First*, though China is a party to the Hague Convention,[8] the Hague Convention's service mandates do not apply where, as here, a plaintiff is seeking provisional relief like a temporary restraining order. *See Fox Corp. v. Media Deportes Mexico, S. de R.L. de C.V.*, 2026 WL 438878, at *10 (S.D.N.Y. Feb. 17, 2026). *Second*, as the *Smart Study* panel itself noted, "the Convention does not apply" when a defendant's address is not known. 164 F.4th at 168; *accord Hague Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters* art. 1, Nov. 15, 1965, 20 U.S.T. 361 (Convention "shall not apply where the address of the person to be served with the document is not known"), https://tinyurl.com/mvpn7tj3. In such a case, the "Rule 4(f)(3) path [is] open." *Smart Study*, 164 F.4th at 168; *see, e.g.*, *Google LLC v. Doe 1*, 2026 WL 353660, at *1 (S.D.N.Y. Feb. 9, 2026) (approving service via email and website publication under Rule 4(f)(3) where Google had been "unable to verify the true identities of the defendants or their physical addresses"). That is the path requested here. *See*, *e.g.*, *id.*; *Google Lighthouse*, Dkt. 18 (same).

[8] *Hague Conference on Private International Law*, Status Table, https://tinyurl.com/36r8u479 (last updated April 21, 2024).

To establish that defendants' addresses are unknown, courts in this district have considered the plaintiff's reasonable diligence to ascertain them. *See Google LLC*, 2026 WL 353660, at *1. To date, Google has not been able—and Google does not anticipate that it *will* be able—to identify Defendants' addresses even with reasonable diligence. (Indeed, remaining undetectable is essential to the Enterprise's success.) Google has already conducted its own investigation into Defendants' activities and hired a cyber-investigation firm to pursue one as well. Google Decl. ¶¶ 28-38; NAXO Decl. ¶ 7. As in past cases against foreign cybercriminals, Google has been unable to verify any addresses associated with these phishing defendants despite these investigative efforts. *See, e.g.*, *Google Darcula*, Dkt. 28 ¶¶ 12-26 (detailing Google's efforts to verify foreign defendants' addresses).

If the Court issues the TRO, Google will serve the order on domain registries to obtain Defendants' addresses, and Google will investigate these addresses with reasonable diligence. *See Google LLC*, 2026 WL 353660, at *1 (holding that Google had demonstrated reasonable diligence "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"). 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.

IV. The All Writs Act Authorizes the Court to Direct Cooperation by Third Parties

The Enterprise uses domains provided by third-party registrars for the fake websites created to perpetrate its fraud. Google's proposed order, if entered by the Court, would direct these third-party registrars to take down and suspend this online infrastructure used by the Enterprise, thereby disrupting its schemes, and to preserve all evidence about Defendants and their websites.

Google Decl. ¶¶ 64-66. This relief would include the disruption of any domains that the Enterprise may use in the future to perpetrate the phishing operations that are currently unknown to Google or that have not yet been created or deployed.

The All Writs Act provides that courts "may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." 28 U.S.C. § 1651(a). This language empowers courts to issue orders to non-parties, and specifically, in "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." *Makekau v. Hawaii*, 943 F.3d 1200, 1205 (9th Cir. 2019) (quoting *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 174 (1977)). Notably, this jurisdiction may "encompass[] even those who have not taken any affirmative action to hinder justice." *Sprint Spectrum L.P. v. Mills*, 283 F.3d 404, 413-14 (2d Cir. 2002) (cleaned up). This "grant of authority to enjoin and bind non-parties to an action" when "needed to preserve the court's ability to … enforce its decision" is "[a]n important feature of the All-Writs Act." *In re Baldwin-United Corp. (Single Premium Deferred Annuities Ins. Litig.)*, 770 F.2d 328, 338 (2d Cir. 1985).

To determine whether the writ requested is "necessary or appropriate" within the meaning of the Act, courts consider whether: (1) the writ "unreasonabl[y] burdens" the third party at issue; (2) the writ is "necessary" or "essential to the fulfillment of the purpose" of a court order; and (3) the third party is "so far removed from the underlying controversy that its assistance could not be permissibly compelled." *N.Y. Tel. Co.*, 434 U.S. at 172-78; *see also United Spinal Ass'n v. Bd. of Elections in City of N.Y.*, 2017 WL 8683672, at *5 (S.D.N.Y. Oct. 11, 2017), *R&R adopted*, 2018 WL 1582231 (S.D.N.Y. Mar. 27, 2018).

The narrowly tailored relief Google requests satisfies these requirements. *First*, requesting these companies to suspend, take down, or transfer the relevant infrastructure imposes minimal burdens. Just as a telephone company "regularly employs [pen register] devices without court order" for its own business purposes, *N.Y. Tel. Co.*, 434 U.S. at 174, domain registrars and web infrastructure companies routinely suspend, terminate, or transfer domain services in the ordinary course of business, *see Chegg, Inc. v. Doe*, 2023 WL 7392290, at *10 (N.D. Cal. Nov. 7, 2023). *Second*, the writ requested is necessary to effectuate the proposed order, the purpose of which is to disrupt the Enterprise's operations and the criminal network that profits from its conduct. Just as the lawful surveillance authorized in *New York Telephone* could not have been accomplished without the participation of the telephone company, reasonable cooperation of the third-party registrars is required here to halt the Enterprise's operation of its scam. *See In re U.S. of Am. for an Ord. Authorizing an In-Progress Trace of Wire Commc'ns Over Tel. Facilities*, 616 F.2d 1122, 1129 (9th Cir. 1980). *Third*, the third parties that maintain this infrastructure are not "so far removed" from the underlying criminal activity that their assistance cannot reasonably be compelled. *See N.Y. Tel. Co.*, 434 U.S. at 174. They control and host the domains that enable the Enterprise to perpetrate its crimes.

Consistent with these principles, courts in this District and across the country have invoked the All Writs Act to grant relief similar to the relief requested here. *See*, *e.g.*, *Google Darcula*, Dkt. 18, at 11-12 (ordering domain registries to ensure that defendant cannot use domains to engage in phishing); *Google Lighthouse*, Dkt. 18, at 11-12 (same); *Google LLC v. Does 1-25*, No. 25-cv-04503 (S.D.N.Y. July 1, 2025), Dkt. 18, at 11-12 (similar); *Starovikov*, 2021 WL 6754263, at *1. To protect the public from the serious threat posed by the Outsider software and Enterprise, it is necessary—and safely within this Court's authority—to order the takedown or transfer of the

domains specified in **Appendix A** to the NAXO Declaration and to authorize Google to take down additional infrastructure in the event that it identifies additional entities associated with or domains used in connection with the Outsider software.

CONCLUSION

Google respectfully requests that this Court grant its motion for a TRO, and an order to show cause why a preliminary injunction should not issue. Google further requests that the Court permit notice of the preliminary injunction hearing and service of the complaint by alternative means.

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 Google LLC's Memorandum of Law in Support of Its Motion for an *Ex Parte* Temporary Restraining Order and Order to Show Cause was prepared using Microsoft Word and contains 8,748 words in accordance with Local Rule 7.1(c).

Dated: June 12, 2026

/s/ *Laura Harris*
Laura Harris