UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC,

Plaintiff,

v.

DOE 1 a/k/a YUCHENG CHANG and DOES 2–25,

Defendants.

Civil Action No.: 1:25-cv-10440-JSR

DECLARATION OF LAURA HARRIS IN SUPPORT OF PLAINTIFF'S MOTION FOR DEFAULT JUDGMENT AND A PERMANENT INJUNCTION

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 ("Google"). I am a member in good standing of the bar of New York. I make this declaration in support of Google's Motion for Default Judgment and a Permanent Injunction and of my own personal knowledge. If called as a witness, I could and would testify competently to the truth of the matters set forth herein.

I. Google Properly Served Defendants.

2. As described more fully below, Doe 1 a/k/a Yucheng Chang and Does 2–25 ("Defendants") have been properly served with the Complaint, ECF No. 1; the summons; the Motion for a Temporary Restraining Order ("TRO"), ECF No. 7; the Memorandum of Law in Support of the Motion for a TRO, ECF No. 13; the Proposed TRO and Order to Show Cause Regarding a Preliminary Injunction, ECF No. 12; all supporting evidence; and the Preliminary Injunction Order, ECF No. 34, pursuant to the means authorized by the Court in the TRO and Preliminary Injunction. *See* ECF No. 37 at Ex. F.

3. A true and correct copy of the Complaint is attached hereto as **Exhibit 1**. A true and correct copy of the summons is attached hereto as **Exhibit 2**. True and correct copies of the Motion for a Temporary Restraining Order, the Proposed TRO and Order to Show Cause Regarding a Preliminary Injunction, and supporting documents are attached hereto as **Exhibit 3**. A true and correct copy of Google's Declaration in Support of Plaintiff's TRO is attached hereto as **Exhibit 4**. A true and correct copy of the Declaration of Laura Harris in Support of Plaintiff's TRO is attached hereto as **Exhibit 5**. A true and correct copy of the Court's Temporary Restraining Order and Order to Show Cause is attached hereto as **Exhibit 6**. A true and correct copy of the Preliminary Injunction Order is attached hereto as **Exhibit 7**.

4. In light of (a) Google's efforts to serve Defendants by email and publication on a publicly available website, magiccatdarculaserviceofprocess.com, beginning on January 4, 2026, (b) widespread news of this case, and (c) Google's disruption of the phishing schemes, Defendants have been on notice of this action since at least January 4, 2026, and likely earlier. Yet, to date, none of the Defendants have appeared in connection with this lawsuit. *See* ECF No. 38.

5. The Defendants against whom default judgment is sought are not infants or incompetent persons. I base this conclusion in part on the fact that Defendants have engaged in sophisticated phishing schemes. I have seen no indication that Defendants are absent or have failed to file responsive pleadings due to present military service.

II. Procedural History

6. On December 17, 2025, Google filed the Complaint in this matter and the Court entered a TRO enjoining Defendants' phishing activities. *See* Ex. 1, ECF No. 18. On January 9, 2025, the Court extended the TRO, and ordered Google to submit supplemental briefing to address the implications of *Smart Study Co. v. Shenzhenshixindajixieyouxiangongsi*, 2025 WL 3672740 (2d Cir. Dec. 18, 2025), on Google's request for alternative service. ECF No. 25. Google submitted its supplemental briefing on January 23, 2026. ECF Nos. 27–30. On February 9, 2026, the Court granted Google's Proposed Preliminary Injunction, Ex. 7, ECF No. 34, and separately issued a Memorandum Order addressing the issue of service and granting Google's request to serve defendants by the alternative means including by email and website publication, ECF No. 33.

7. On March 13, 2026, Google filed a request for Entry of Default, *see* ECF No. 36, with a Declaration of Laura Harris in Support of Google's Request for Entry of Default, *see* ECF No. 37, and the Clerk of the Court entered a Certificate of Default on March 16, 2026, *see* ECF No. 38. A true and correct copy of Google's Request for Entry of Default is attached hereto as **Exhibit 8**. A true and correct copy of the Declaration of Laura Harris in Support of Google's

Request for Entry of Default is attached hereto as **Exhibit 9**. A true and correct copy of the Certificate of Default is attached hereto as **Exhibit 10**.

III. Service of Process

8. The Court found good cause to grant alternate service by email, mail, and publication on a publicly available website, pursuant to Rule 4(f)(3), and, as described more fully below, the Defendants have been properly served pursuant to the means authorized by the Court.

a. Identification of Defendants' Email Addresses & Phone Numbers

9. In connection with the disruption of the botnet, Google served the Court's Temporary Restraining Order and Order to Show Cause ("TRO") on the third-party internet domain registrars (the "registrars") for the domains listed in Appendix A. Many of the registrars provided contact information associated with the relevant accounts, including the email addresses and mailing addresses used to register the domains in question. Google's own investigation identified additional email addresses associated with the Enterprise.

10. Pursuant to the Court's order, King & Spalding used this contact information to effectuate service on the Defendants.

11. I oversaw Google's efforts to provide service and notice to the Defendants through the multiple channels identified below.

b. Service by Email

12. Google attempted to effectuate service by email, as authorized by the Court. Through its own investigation, Google identified 5 email addresses associated with domains listed in Appendix A and Google also received from the registrars 26 email addresses used to register domains listed in Appendix A. I oversaw the process of sending notice of this lawsuit to these email addresses.

13. Each email attempting to effectuate service was sent by an attorney at King & Spalding with the following text:

> A lawsuit has been initiated against you in the United States District Court of the Southern District of New York. The following link contains copies of the restraining order, complaint, and related filings.
>
> magiccatdarculaserviceofprocess.com
>
> King & Spalding LLP

14. King & Spalding received delivery failure notifications for four of the email addresses noting either that there was a problem with the recipients mailbox or that the address may not exist.

15. King & Spalding attempted to effectuate service by email, as described above, on January 4, 2026, at approximately 7:26 p.m. ET.

16. On February 9, 2026, King & Spalding attempted to effectuate service of additional filings, including the Preliminary Injunction Order issued by the Judge that same day, to the email addresses previously mentioned. King & Spalding received delivery failure notifications for 10 of the 31 email addresses noting that either the email address may not exist or was inactive.

17. On February 19, 2026, King & Spalding attempted to effectuate service of additional filings, including the Summons issued by the Clerk of Court that same day, to the email addresses previously mentioned. King & Spalding again received delivery failure notifications for 10 of the 31 email addresses.

c. Service by Publication

18. Google also attempted to effectuate service by publication through a publicly available website, as authorized by the Court.

19. On January 4, 2026, Google published the website magiccatdarculaserviceofprocess.com, which contains links to all relevant pleadings and orders as well as contact information for Google's counsel. That website is routinely updated.

20. The website prominently displays the following text:

> Plaintiff Google LLC ("Google") has sued Defendants Does 1-25 associated with the Internet domains listed in the pleading set forth below. Google alleges that Defendants have deployed a phishing-as-a-service model to facilitate and execute phishing attacks designed to steal personal and financial information, and Defendants have misused Google trademarks in their scheme. Google alleges that, through these actions, the Defendants have violated federal law. Google sought and received a temporary restraining order enjoining the Defendants from these and other activities and directing the third parties associated with Defendants' Internet domains to take all steps necessary to disable access to and operation of Magic Cat/Darcula-associated domains. Google intends to seek a preliminary injunction and other equitable relief. Full copies of the complaint, related filings, and orders from the Court are available below.
>
> NOTICE TO DEFENDANT: READ THESE PAPERS CAREFULLY! A hearing to show cause why the Court should not enter a Preliminary Injunction will be held on January 9, 2026 at 10 a.m.
>
> You must "appear" in this case or the other side will win automatically. To "appear" you must file with the court a legal document called a "motion" or "answer." The "motion" or "answer" must be given to the court clerk or administrator within 21 days of the date of first publication specified herein. It must be in proper form and have proof of service on Google's attorney, Laura Harris, King & Spalding LLP, 1290 Avenue of the Americas, 14th Fl., New York, NY 10104-0101. If you have questions, you should consult with your own attorney immediately.

21. A link to this website was also included in each service of process email. Attached hereto as **Exhibit 11** is a true and correct copy of a printed copy dated March 2, 2026, of the publicly available website, magiccatdarculaserviceofprocess.com.

IV. Additional Means of Notification

22. Upon information and belief, the Defendants also have actual notice of this proceeding given the impact of the TRO, the Preliminary Injunction Order, and Google's disruption efforts thereunder.

23. Following the Court's issuance of the TRO on December 17, 2025, Google began its efforts to disrupt the Internet domains associated with the Darcula Enterprise. As detailed in the Court's Preliminary Injunction Order, *see* Ex. 7, ECF 34, Google's efforts have led to the suspension or disruption of 325 domains associated with the Darcula Enterprise.

24. Many news websites have published stories concerning this litigation. Below are just a few examples of this media coverage detailing the claims against the Defendants:

- Kevin Collier, *Google sues alleged Chinese scam group behind massive U.S. text message phishing ring*, NBC News (Dec. 17, 2025), https://www.nbcnews.com/tech/security/google-sues-chinese-scam-ring-e-zpass-usps-phishing-texts-rcna249469.

- Jeff Stone, *Google Sues Chinese 'Darcula' Group Over Alleged Phishing Scheme*, Bloomberg (Dec. 17, 2025), https://www.bloomberg.com/news/articles/2025-12-17/google-sues-chinese-darcula-group-over-alleged-phishing-scheme.

- Steve Weisman, *Google Sues Darcula: How The Tech Giant Is Using The Courts To Fight Cybercrime*, Forbes (updated Dec. 27, 2015), https://www.forbes.com/sites/steveweisman/2025/12/26/googles-sues-darcula-how-the-tech-giant-is-using-the-courts-to-fight-cybercrime/.

- Gintaras Radauskas, *Google sues another Chinese scam group over large phishing scheme*, Cybernews (Dec. 18, 2025), https://cybernews.com/security/google-cybercrime-chinese-gang-darcula/.

- Mudit Dube, *Google Sues Chinese Group Behind Massive Phishing Scam*, NewsBytes (Dec. 18, 2025), https://www.newsbytesapp.com/news/science/google-sues-chinese-group-behind-us-text-message-phishing-ring/story.

V. Defendants' Ongoing Conduct

25. Without a permanent injunction, Defendants will regain access to the domains Google has disrupted and continue to participate in cybercriminal activities through the Darcula Enterprise. These actions will continue to cause harm to Google, its customers, and the public.

VI. Damages

26. Google's Complaint sought a judgment awarding (i) actual damages, (ii) enhanced, exemplary, and special damages, and (iii) attorneys' fees and costs, *see* Ex. 1, ECF No. 1. Google

has withdrawn its request for monetary damages in connection with its motion for Default Judgment and a Permanent Injunction.

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

Executed on March 18, 2026, in New York, New York.

/s/ Laura Harris
Laura Harris

EXHIBIT 1

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC, *Plaintiff,* v. DOE 1 a/k/a YUCHENG CHANG and DOES 2–25, *Defendants.*	Civil Action No.:

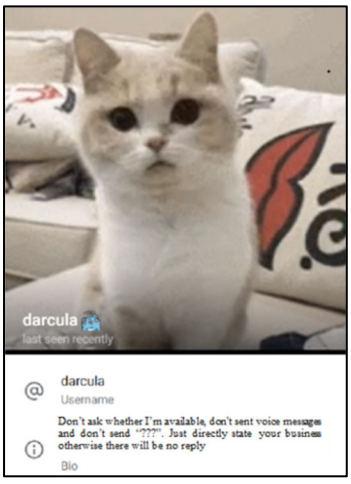
COMPLAINT FOR DAMAGES AND INJUNCTIVE RELIEF

Plaintiff Google LLC ("Google"), by and through its attorneys, brings this Complaint against Defendants for injunctive relief and damages. Google alleges as follows:

INTRODUCTION

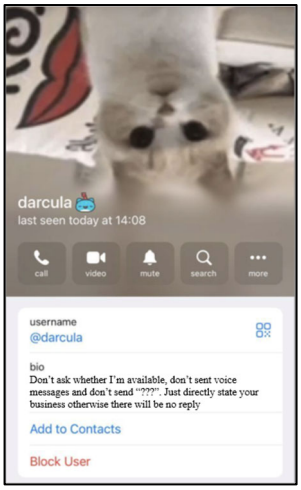
1. Defendants are a group of foreign cybercriminals who design and execute novel "phishing" attacks,[1] using artificial intelligence ("AI") technology to mimic legitimate websites and dupe victims into disclosing personal and financial information. These attacks have swindled millions of victims globally, including Google customers, and have exploited Google's reputation through the unauthorized use of its trademarks and impersonation of Google's services. To combat these cybercrimes, Google is seeking an injunction to disrupt Defendants' criminal enterprise and the infrastructure on which it relies.

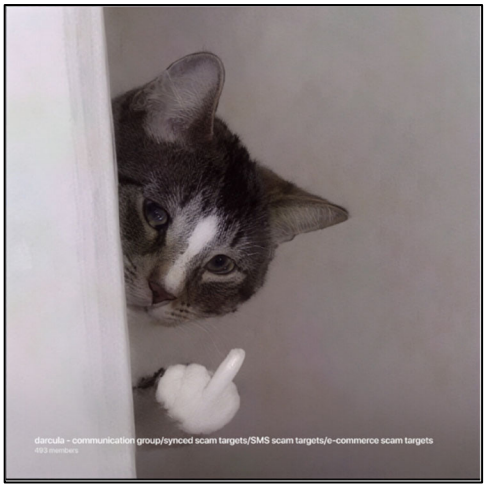
2. In 2023, Defendants developed and deployed an end-to-end phishing software known as "Magic Cat," a "phishing for dummies" kit that provides the technical infrastructure to create and deploy large-scale phishing attacks for those with little technical know-how. Operating online under the alias "Darcula," Defendants are known for their signature use of cat images as profile pictures.[2]



[1] A "phishing" attack is a form of cyberattack that dupes victims into clicking on malicious links with false messages, such as purported notices about a lost package or unpaid toll.

[2] Erlend Leiknes & Harrison Sand, *Exposing Darcula: a rare look behind the scenes of a global Phishing-as-a-Service operation*, Mnemonic (May 4, 2025), https://tinyurl.com/537tm5bs.





3. Magic Cat's developers and their network of collaborators and co-conspirators—including those who deploy Magic Cat to execute phishing campaigns—are referred to herein as the "Darcula Enterprise" or the "Enterprise."

4. Magic Cat is not simply a back-end technical tool; the software provides a suite of easy-to-use resources to create, deploy, and monitor criminal phishing campaigns on a user-friendly interface. The latest version of the software features cutting-edge AI technology capable of creating a fake version of any website in minutes, tools to bring the websites online, administrative functionality to track and store stolen data, and advanced troubleshooting and customer support features, all designed and maintained to evade detection and lead victims to believe they are transacting with legitimate businesses and government entities.

5. Using Magic Cat, Enterprise members create phishing campaigns and send mass text messages to potential victims—for example, luring them to sign up for what purports to be (but is not) a free trial of Google's YouTube Premium service through a spoofed version of Google's YouTube Premium sign-up webpage, or warning them (falsely) that their bank account is compromised. Those fake websites are nearly indistinguishable from the real thing and often bear the hallmarks of legitimate sites, even purporting to permit victims to sign in through a Google

account, and tricking victims into turning over their personal information, credit card numbers, and other sensitive financial data, which the Darcula Enterprise uses to steal victims' money or sells to other criminal actors.

6. At its height, researchers estimated that the Enterprise was responsible for upwards of 70 to 80% of all phishing text messages, with at least 600 cybercriminals coordinating to deploy and execute its phishing schemes to unsuspecting victims across the globe.[3] Over the course of just seven months, the Darcula Enterprise stole nearly 900,000 credit card numbers from individuals around the world, including nearly 40,000 credit card numbers from individuals in the United States alone.

7. Today, thanks to the work of the cybersecurity experts and journalists who have alerted the public to the Darcula scheme,[4] the Enterprise has reduced its profile and no longer openly markets its software. But Google's investigation has revealed that new Magic Cat-linked phishing websites continue to be created daily and that significant portions of the Enterprise's cyber infrastructure remain in place, ready to be redeployed at any moment.

8. The Enterprise preys upon the public's trust in Google, a leader in the technology space, by misappropriating Google branding, including by incorporating Google's trademarks (as further defined herein, Google's "Marks") into fraudulent websites including by impersonating Google's YouTube platform. The Enterprise interferes with Google's relationships with its users (and potential users), harms Google's reputation, impairs the value of Google's products and services, and forces Google to devote substantial resources to investigate and combat the Enterprise's criminal activity, causing Google financial harm and undermining customer goodwill.

[3] Martin Gundersen, *Inside the Scam Network*, NRK (May 4, 2025), https://tinyurl.com/5n6cp2jd.
[4] *See id.*

9. Google therefore brings this action under the Racketeer Influenced and Corrupt Organizations Act ("RICO"), the Lanham Act, and the Computer Fraud and Abuse Act ("CFAA") against Defendants to disrupt their criminal enterprise and prevent it from causing further harm, and to recover damages.

PARTIES

Plaintiff

10. Plaintiff Google LLC is a Delaware limited liability company with its principal place of business at 1600 Amphitheatre Parkway in Mountain View, California.

11. Google is a leading technology company that offers a wide variety of services to organize the world's information and make it universally accessible and useful. Its search engine, accessible at www.google.com, is the most widely used internet search service in the world. Gmail, a free email service used by more than 1.5 billion people worldwide, includes a variety of revolutionary and innovative features, including an industry-leading two full gigabytes of email storage; email message threading; fast, precise search of emails using an integrated Google search engine; and freedom from pop-up or irrelevant advertising. Google also offers YouTube, an online video sharing platform that millions of people use to share and watch videos each day. While YouTube is a free platform, Google also offers a premium version of YouTube on a subscription model through which subscribers can access YouTube with no advertisements, download YouTube videos for offline viewing, and watch YouTube videos "in the background"—in other words, while using other applications on mobile devices.

12. Google operates numerous products, platforms, and services, many of which are relevant here:

a. **Android**: Android is an operating system created by Google that is designed to run on mobile devices, such as smartphones or tablets. Google has both a proprietary

version that is used for official Google devices and has also released a free version as open-source software. In this Complaint, where we refer to "Android," we refer to Google's proprietary version.

b. **Chrome**: Chrome is a web browser created and operated by Google that runs on various operating systems, including on personal computers, smartphones, and tablets.

c. **Gmail**: Gmail is an email service.

d. **Google Search**: Google Search is an internet-based search engine that allows users to search for publicly accessible documents and websites indexed by Google's servers.

e. **Google Pay**: Google Pay is a digital wallet and online payment system that allows users to make safe and secure payments, send money, and manage their finances using their smartphones, tablets, or computers. Google Pay has built-in authentication, transaction encryption, and fraud protection to keep customers' money and personal information safe.

f. **Google Play**: Google Play is the official app store for certified devices running on the Android operating system, allowing users to browse and download apps developed with the Android software development kit and published through Google. Google Play also serves as a digital content store that offers millions of apps, games, books, and other products to more than 2.5 billion monthly users across over 190 markets worldwide.

g. **Rich Communication Services ("RCS"):** RCS chats let users send messages and share files, including high-resolution photos, over mobile data and Wi-Fi. Messages

sent via RCS chats use the RCS protocol, an industry standard for carrier messaging, and Google's RCS infrastructure. RCS chats between Google Messages users are end-to-end encrypted by default to keep users' conversations secure.

h. **YouTube**: YouTube is an online video sharing platform. YouTube Premium provides premium, ad-free access to YouTube content with a subscription and can be purchased online.

13. Google strives to provide its users worldwide with safe and secure platforms. Google has therefore invested substantial resources to identify, understand, and ultimately disrupt harmful phishing operations like those deployed by the Darcula Enterprise.

Defendants

14. Defendant Doe 1 a/k/a Yucheng Chang is an individual who has conspired with other Defendants to engage in a pattern of racketeering activity. He has played a significant role in the development and maintenance of Magic Cat, participated in the management and operation of the Darcula Enterprise's phishing schemes, and committed criminal acts that have caused harm to Google, its users, and numerous others, as described below. He resides in China.

15. Defendants Does 2–25 are other individuals or entities who have conspired to engage in a pattern of racketeering activity. They have each participated in the operation or management of the Darcula scheme and engaged in criminal acts that have caused harm to Google, its users, and countless others. Defendants reside in China or other foreign countries.

16. At this time, Google does not know the true names and capacities of the Doe Defendants. Each of these Defendants is responsible in some manner for the conduct alleged, having agreed to become part of the Darcula Enterprise.

17. Google is presently aware of multiple connected Doe actors within the Darcula Enterprise. It is not clear precisely how many actors or groups comprise the Enterprise; the Doe numbers are meant to be representative. All the threat actors are connected to one another through overlapping infrastructure and historical and current business ties. The threat actors' misconduct is described in more detail below.

JURISDICTION AND VENUE

18. This Court has federal-question subject matter jurisdiction (28 U.S.C. § 1331) over Google's Lanham Act, RICO, and CFAA claims pursuant to 15 U.S.C. § 1051 *et seq.*,18 U.S.C. § 1961, and 18 U.S.C. § 1030, respectively.

19. Defendants are subject to personal jurisdiction in this district, and the exercise of jurisdiction over Defendants is proper pursuant to 15 U.S.C. § 1121; 18 U.S.C. § 1965; and N.Y. C.P.L.R. §§ 301 and 302. Defendants have transacted business and engaged in unlawful and tortious conduct in the United States and in New York that gives rise to Google's claims. Defendants also have engaged in intentional, wrongful, illegal, and/or tortious acts, the effects of which Defendants intended to and knew would be felt in the United States and New York. Among other things, Defendants have used Google logos as part of spoofed websites used to solicit victims' personal financial information in New York and throughout the United States and have directed multiple forms of communication to devices in New York and throughout the United States for the purpose of planning and carrying out their conspiracy and fraud. Defendants were aware of the effects in the United States and New York of those acts; the activities of their co-conspirators and agents were to the benefit of Defendants; and their co-conspirators and agents were working at the direction, under the control, at the request, and/or on behalf of Defendants in committing those acts.

20. Defendants have affirmatively directed actions at the United States, including the Southern District of New York, by attempting to and successfully phishing personal financial information from hundreds of victims in New York, including at least one hundred victims in the Southern District of New York. Defendants have aimed each of these illegal activities at individuals within the Southern District of New York.

21. Defendants have also intentionally targeted and harmed Google, a company based in the United States.

22. Venue is proper in this judicial district under 28 U.S.C. § 1391(c) because Defendants are not residents of the United States and may therefore be sued in any judicial district. Venue is also proper in this judicial district under 28 U.S.C. § 1391(b) and 18 U.S.C. § 1965 because a substantial part of the events or omissions giving rise to Google's claims occurred in this judicial district, because a substantial part of the property that is the subject of Google's claims is situated in this judicial district, because a substantial part of the harm caused by Defendants has occurred in this judicial district, and because Defendants transact their affairs in this judicial district. Defendants engage in conduct in New York and utilize instrumentalities located in this judicial district to carry out acts alleged herein.

FACTUAL ALLEGATIONS

Phishing, Smishing, and Phishing-as-a-Service

23. As personal devices and email have replaced telephone lines and traditional mail, criminal activity has likewise evolved and is leveraging those tools to reach more victims with less effort. One of the most common forms of internet-based criminal schemes is phishing. The sophistication and reach of phishing schemes have grown dramatically—cybercriminals are now

sending an estimated 3.4 billion phishing emails every day.[5] Phishing has become the most ubiquitous form of criminal fraud.

24. "Phishing" is a type of cyberattack in which threat actors impersonate well-known brands, government agencies, or known individuals within an organization to trick individuals into disclosing their sensitive information, like passwords, credit card numbers, or banking information. The attacker sends victims a deceptive message in an email or other electronic communication that is crafted to appear trustworthy. The phishing message asks the target to click a link or fill out a form to transmit their personal data, which threat actors then steal for their own criminal use.

25. "Smishing" is a type of phishing where threat actors use text messages (such as SMS or RCS messages) to trick victims into turning over their information. The threat actors often use urgent language to cause the recipient to fear that if they do not act immediately to remediate the (fake) issue, there will be consequences. These messages, which target thousands of phone numbers at a time, encourage recipients to click on a malicious link that leads to a fraudulent phishing website.

26. Smishing is especially nefarious because victims tend to "place more trust in these types of messages than in email."[6] That trust, paired with the heightened sense of urgency conveyed by these messages, "results in a significantly higher expected conversion rate than email … and other techniques the actors could use."[7]

---

[5] Sienna Arellano & Ian Kilty, *The Phishing Business Model*, Colo. State Univ. System: Info. Tech. (Feb. 17, 2025), https://tinyurl.com/psxum3se.
[6] Resecurity, *Smishing Triad Is Now Targeting Toll Payment Services in a Massive Fraud Campaign Expansion* (Apr. 8, 2025), https://tinyurl.com/8jsb3dm7.
[7] *Id.*

27. Once threat actors have sensitive information in hand, they can use it to access victims' email accounts, bank accounts, and more. Scammers often load the stolen payment cards to digital wallets—like Google Wallet—on mobile devices and then sell the mobile devices to others. Scammers can also relay new stolen card information in real time to devices used by co-conspirators to make in-person purchases, a practice known as "ghost tapping."[8] Some recent law enforcement actions have identified criminal networks using phones loaded with stolen credit card information and tap-to-pay functionality to purchase gift cards in bulk.[9] Other groups simply purchase their own tap-to-pay machines and configure them to deposit payments into their own bank accounts, using customer cards to make payments directly to themselves.[10] Still others use stolen brokerage firm credentials to perpetrate a modern iteration of a "pump and dump" scheme, pre-purchasing shares of a particular stock and then using compromised brokerage accounts to purchase large volumes of the stock, inflating the price before they liquidate their original holdings.[11]

28. These schemes have proven to be enormously profitable, meaning that the infrastructure necessary to execute them has become a commodity as well. So-called phishing-as-a-service ("PhaaS") is a business model that distributes software and support services to facilitate phishing, making it relatively easy for those without technical expertise to create and execute a

[8] Insikt Group, *Ghost-Tapping and the Chinese Cybercriminal Retail Fraud Ecosystem*, Recorded Future (Aug. 14, 2025), https://tinyurl.com/4fb77c7e.
[9] Josh Jarnagin, *Knox County Detectives Investigating 'Ghost Tap' Credit Card Fraud*, WVLT8 (May 31, 2025), https://tinyurl.com/bdffxm4y; *see also* Singapore Police Force, *Unauthorised Card Transactions Made Using Contactless Payment Methods in Singapore* (Feb. 17, 2025), https://tinyurl.com/mwx6nv76.
[10] *See* Brian Krebs, *How Phished Data Turns into Apple & Google Wallets*, KrebsOnSecurity (Feb. 18, 2025), https://tinyurl.com/37a3fzps.
[11] *See* Brian Krebs, *Mobile Phishers Target Brokerage Accounts in 'Ramp and Dump' Cashout Scheme*, KrebsOnSecurity (Aug. 15, 2025), https://tinyurl.com/4mv37y8b.

phishing campaign. The software, sometimes referred to as a "phishing kit," provides the infrastructure necessary to create fake websites (or other platforms), send bulk text messages or emails to victims, and collect and store stolen personal and financial information. For example, a phishing kit may contain ready-made website templates that closely resemble legitimate websites. Phishing kits enable criminals without technical expertise to engage in phishing and smishing, to reach larger numbers of targets, and to mimic a greater number of websites, making these types of attacks much more frequent and effective.

29. The PhaaS model also makes stopping phishing attacks more difficult. "Catching the person who carried out the attack does not put an end to the story. You will still have to catch the guy who designed the phishing kit and the one who provided it."[12]

The Magic Cat Phishing Software

30. First identified in July 2023,[13] Magic Cat is a bundle of software tools that enables threat actors to create spoofed text messages and websites through which unsuspecting victims—who believe the text or website is legitimate—disclose their personal and financial information. Magic Cat includes templates of fraudulent phishing websites that are designed to resemble legitimate websites.

31. The Magic Cat software package[14] includes two integrated components: (1) front-end software that is used to create, design, and edit phishing websites, and to configure

[12] Andreea Chebac, *What Is Phishing-as-a-Service (PhaaS) and How to Protect Against It*, Heimdal (July 7, 2025), https://tinyurl.com/5n6mp39p.
[13] Jessica Lyons, *Darcula adds AI to its DIY phishing kits to help would-be vampires bleed victims dry*, The Register (Apr. 25, 2025), https://tinyurl.com/ywban2f6; Ravie Lakshmanan, *Darcula Phishing Network Leveraging RCS and iMessage to Evade Detection*, The Hacker News (Mar. 28, 2024), https://tinyurl.com/2s4fhcnj.
[14] This software is sometimes referred to as "Darcula" software; however, users typically refer to the entire software package as "Magic Cat," the term used to refer to the software herein.

certain aspects of the phishing kit; and (2) a server-based program that is used to deploy phishing sites and collect stolen information from victims who are tricked into entering credit card information.

32. Much like legitimate software, Magic Cat is designed for ease of use. From the Magic Cat platform, a threat actor can generate a spoofed website and phishing "bait" messages, launch their phishing campaign, collect personal and financial data submitted by phishing victims, transform stolen financial information into virtual credit cards for immediate criminal use, and even monitor the relative success of their schemes through a sleek performance dashboard.

33. The earliest versions of Magic Cat offered around 200 phishing templates that spoof the websites of well-known brands in over 100 countries.[15] At the height of its use, it featured more than 300 templates.[16] Many of Magic Cat's templates are designed to target U.S. victims, such as websites spoofing the webpages of the Internal Revenue Service and the U.S. Postal Service ("USPS").

34. Members of the Enterprise distribute Magic Cat via several Telegram channels,[17] including the @darcula_channel, and on various sites on the dark web.

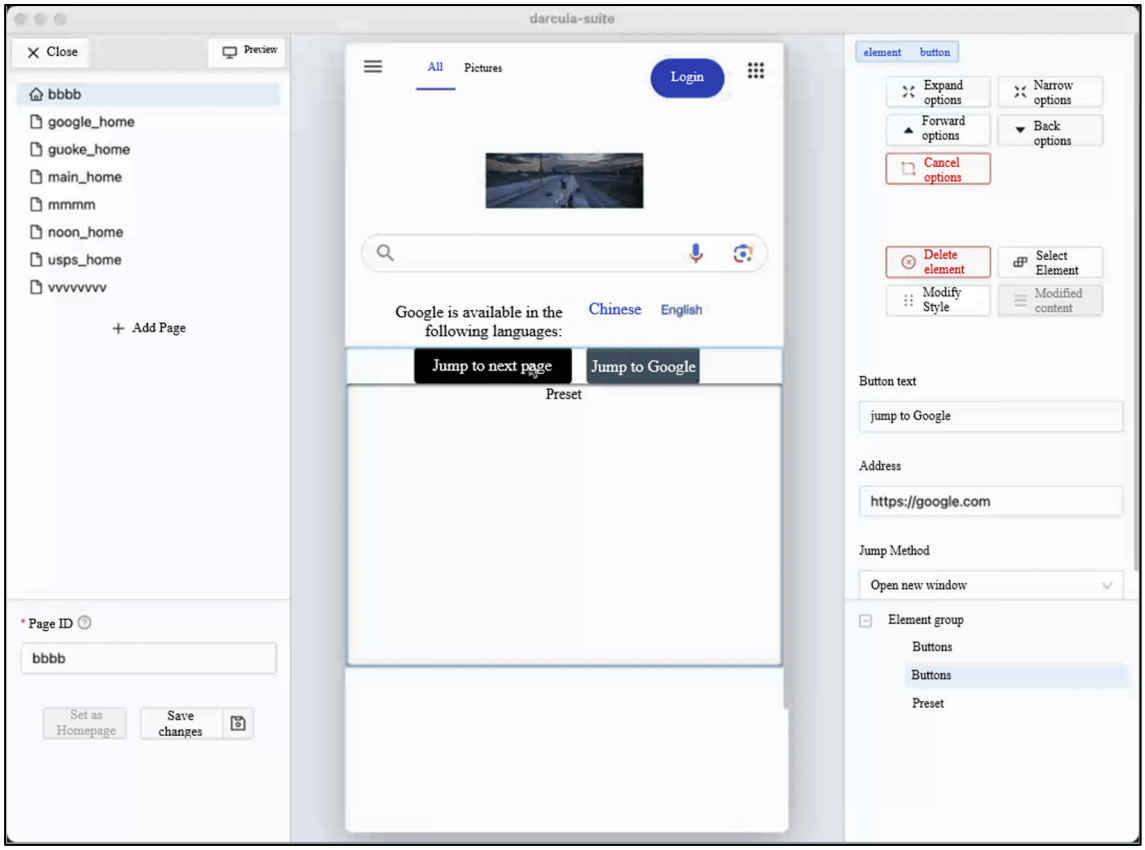
35. Earlier this year, the Darcula Enterprise debuted an even more pernicious version of the Magic Cat software. This latest iteration integrates generative AI and other features that allow the Enterprise to create near-perfect duplicates of virtually any legitimate website in minutes, without any programming knowledge. Members of the Enterprise simply input the URL of a

[15] Ravie Lakshmanan, *Darcula Phishing Network Leveraging RCS and iMessage to Evade Detection*, The Hacker News (Mar. 28, 2024), https://tinyurl.com/2s4fhcnj.
[16] Martin Gundersen, *Inside the Scam Network*, NRK (May 4, 2025), https://tinyurl.com/5n6cp2jd.
[17] Telegram is a free messaging service with over one billion monthly active users. Telegram channels are designed for one-way information sharing, where channel administrators can post in the channel to share information with channel members.

legitimate website and Magic Cat's AI tools collect the website's data and generate a fraudulent version. Those spoofed websites include logos and features of the real websites, including, for example, Google Play and YouTube logos, and links to those sites and features.

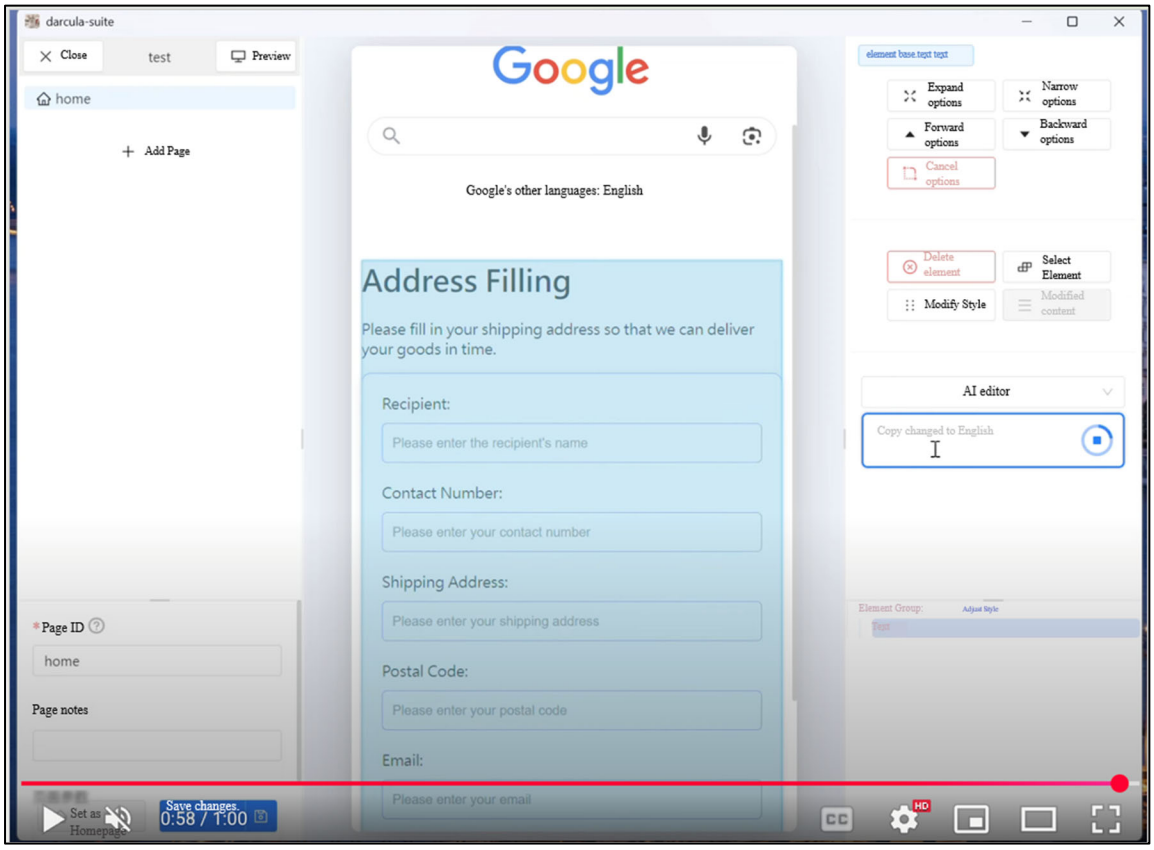
36. Magic Cat's built-in AI tool dramatically increases the threat posed by the Darcula Enterprise. Now, threat actors are not confined to the software's templates in determining which websites to duplicate in their phishing campaigns—they can mimic any website they believe will most effectively dupe their victims into providing personal and financial information.

37. In fact, Magic Cat includes a tutorial that demonstrates how to use the software. Those tutorial images show the software being used to spoof Google's homepage, Google.com, as shown below.



38. The Enterprise released another tutorial in April 2025 that again used a spoofed version of Google's homepage, Google.com, to demonstrate Magic Cat's new AI functionality.

To create a website that mimics Google's homepage, the Enterprise member copies data from Google's homepage into Magic Cat and then uses an AI tool to create a form purporting to collect address information. The form includes a request to "[p]lease fill in your shipping address so that we can deliver your goods in time." The Enterprise member can create the fillable form in Chinese and then use the Magic Cat "AI editor" box to translate the form into English, or another language of its choosing.



39. After generating a spoofed website, the Enterprise member sends the website's URL to targets through text messages, often called "bait" messages. Magic Cat's "bait" messages are deployed in text messages sent via Apple iMessage, RCS (the platform used by Google Messages), and SMS.

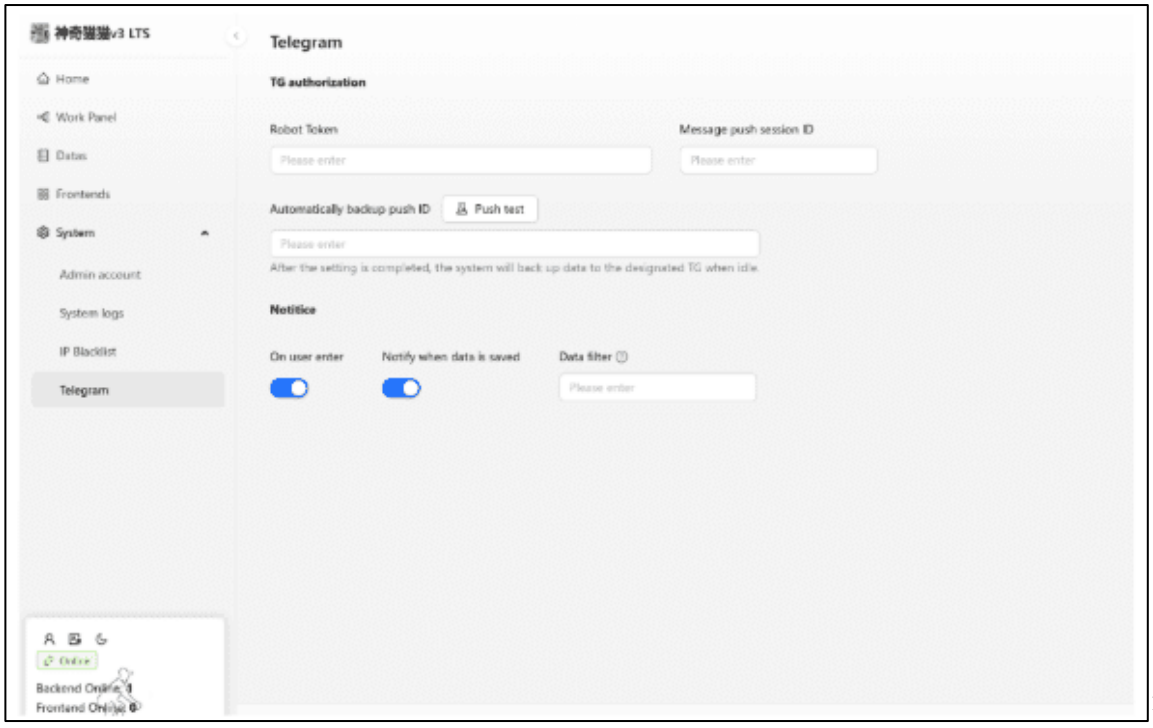
40. Using iMessage and RCS messages lends a veil of legitimacy to Magic Cat smishing attacks (where, for example, iMessage users may be more suspicious of "green" SMS

messages than "blue" iMessages), while simultaneously evading certain filters leveraged by SMS operators to block smishing messages.

41. Once the Enterprise member has used Magic Cat to generate and deploy "bait" in the form of phishing messages directing victims to fraudulent links, Magic Cat also provides the perpetrator real-time access to data entered by victims into the phishing websites by tracking the victim's keystrokes and relaying that information to the Enterprise member as the victim types.[18]

42. Magic Cat notifies the threat actor with a voice alert when a victim has accessed their fraudulent website and streams personal data to the threat actor as it is entered into the site.

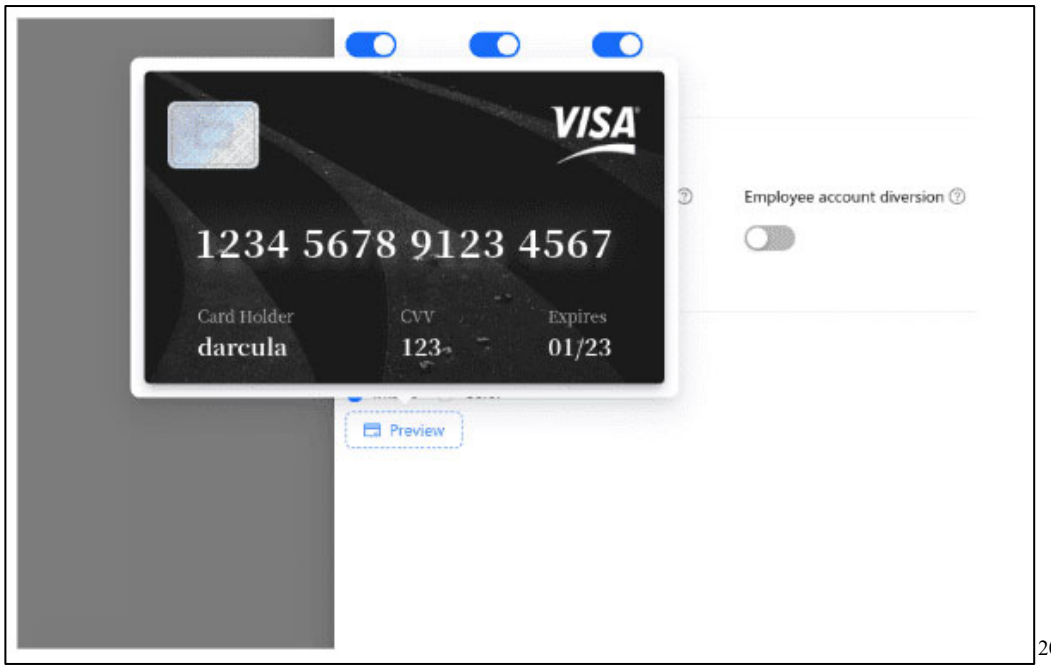
43. Magic Cat also offers integration with Telegram, allowing threat actors to receive notifications through that platform as well:



[19]

[18] Erlend Leiknes & Harrison Sand, *Exposing Darcula: a rare look behind the scenes of a global Phishing-as-a-Service operation*, Mnemonic (May 4, 2025), https://tinyurl.com/537tm5bs.
[19] Harry Freeborough, *The Bleeding Edge of Phishing: darcula-suite 3.0 Enables DIY Phishing of Any Brand*, NetCraft (Feb. 20, 2025), https://tinyurl.com/vmtu8h7h.

44. This suite of features allows cybercriminals with minimal technical expertise to steal victims' credit card numbers, financial account information, and personal data. But Magic Cat goes a step further in facilitating digital theft. Its program allows users to turn the stolen information into clones of victims' credit cards that can be added to digital wallets, as pictured below.



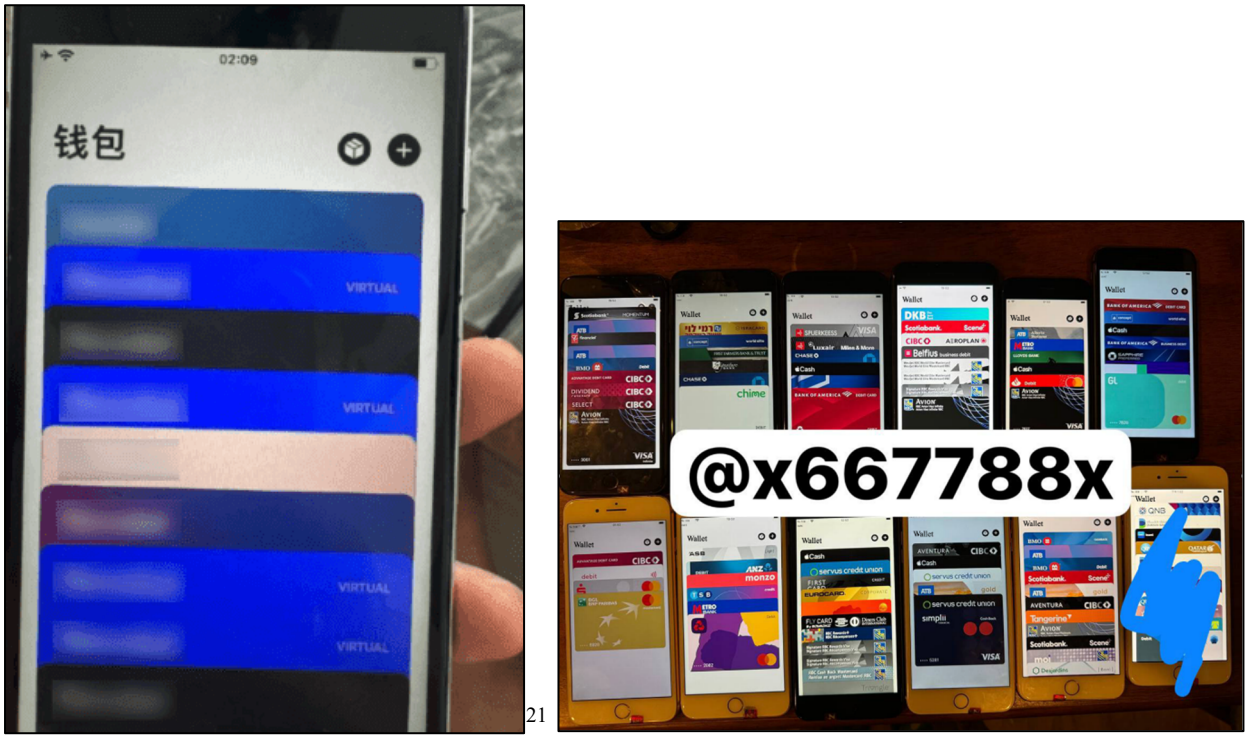
[20]

45. Members of the Darcula Enterprise commonly load these stolen cards onto burner phones they sell through illicit channels or use themselves for either online or in-person purchases using digital wallets like Google Pay's tap-to-pay technology.

46. Enterprise members have posted images to the Enterprise's Telegram community boasting about how they have stolen numerous credit cards, loaded those cards onto burner phones, and then offered those phones for sale. The photo on the left below is a picture that a member of

[20] *Id.*

the Enterprise posted that depicts a burner phone loaded with twenty stolen credit cards. The photo on the right depicts a dozen phones with stolen cards loaded onto digital wallets.



[21]

The Darcula Enterprise

47. The Darcula Enterprise includes several connected threat actor groups that design and implement complex criminal schemes targeting the general public. Although different members of the Enterprise play different roles, they all collaborate to execute phishing schemes that rely on the Magic Cat phishing software. None of the Enterprise's schemes can generate revenue without the cooperation of these groups. All the threat actor groups are connected to one another through historical and current business ties, including through their use of Magic Cat and the online community supporting its use, as described below. Although certain Enterprise members

[21] *Id.*

may serve multiple roles, the Enterprise is generally composed of members who participate in the following groups:

48. **The Developer Group:** The Developer Group supplies the phishing software, templates, and updates.

49. It includes the individuals or entities that develop and maintain Magic Cat by designing the software, architecture, and user interface, writing code to carry out its functions, and troubleshooting the software to ensure it works properly. The Developer Group is also responsible for providing ongoing maintenance, pushing out regular software updates, and integrating new features into the software.

50. The Developer Group includes, but is not limited to, individuals who operate under the Darcula alias, including Defendant Doe 1 a/k/a Yucheng Chang. When researchers contacted an email address associated with Chang, an individual acting under the alias "Lao Liu" confirmed that Chang "is employed by our company," that Chang was "one of the founders of Magic Cat," that "there are many people behind the program," and that Chang is "just one of the technologists who developed the program."[22] The individual also stated that while Chang "sells the most," "the income belongs to the company."[23]

51. In addition to performing routine maintenance on Magic Cat and providing troubleshooting and support tools to better enable threat actors to perpetrate phishing schemes, the Developer Group has launched two major upgrades to Magic Cat, dubbed "V2" and "V3."

[22] OSINT Industries Team, *Darcula and the Magic Cat: How OSINT Unmasked A Phishing Tycoon*, OSINT (Aug. 12, 2025), https://tinyurl.com/ypzjyuyu; Martin Gundersen, *The Hunt for Darcula*, NRK (May 8, 2025), https://tinyurl.com/42bj5esj.
[23] Martin Gundersen, *The Hunt for Darcula*, NRK (May 8, 2025), https://tinyurl.com/42bj5esj.

52. In V2, the Developer Group included hundreds of preloaded phishing templates for fraudulent websites mimicking U.S. government websites as well as the websites of major U.S. corporations.

53. In V3, the Developer Group added website customization and generative AI tools allowing Enterprise members to generate custom phishing templates, and redesigned the administrative dashboard to make it even more user-friendly.

54. **The Administrative Group:** The Administrative Group runs an online community designed to facilitate collaboration among Enterprise members and to recruit new members.

55. Part of the appeal of the Magic Cat software is the ease with which someone with little technical expertise can purchase the software and immediately deploy a wide array of phishing attacks. That user-friendly appeal is enhanced by the tutorials, easily accessible instructions, technical support, and online community hosted on Telegram by the Administrative Group.

56. Between 2023 and early 2025, the Administrative Group created and managed a Telegram-based online community that was used to recruit new members of the Enterprise and to assist Enterprise members in using Magic Cat to carry out phishing attacks.

57. Some members of the Administrative Group also operate under the Darcula alias.

58. In one Darcula Telegram channel (@darcula_channel), members of the Administrative Group posted announcements regarding software updates as changes and improvements to the software were made available.

59. For example, on May 10, 2024, a member of the Administrative Group posted a video tutorial walking through the Magic Cat software features along with the post, "[t]here's a

little bit to look forward to, many parts have recently been standardized and rectified, laying the groundwork for the direction of future development."

60. The Administrative Group also used the @darcula_channel Telegram channel to promote and distribute resources for its phishing operations. For example, on July 2, 2023, a member of the Administrative Group posted, "Selling worldwide online data. Contact @pk520520 if needed."

61. On another Darcula-linked Telegram channel (@n9999n), members of the Enterprise record transactions they made. Additional channels have been used to promote Magic Cat by disseminating demonstrations of the software, to connect Enterprise members to allow them to collaborate on phishing schemes, and to enable Enterprise members to boast to other members about the success of their schemes.

62. **The Data Broker Group:** Members of the Data Broker Group provide the list of targets.

63. These individuals or entities supply lists of potential victims' contact information to other members of the Darcula Enterprise, ensuring the wide reach of its many phishing schemes. Members of this group identify and compile contact information for potential victims and distribute the information for use in phishing attacks. One member of the Data Broker Group is user @pk520520, who shares international telephone numbers and contact information to Magic Cat scammers to enable their mass phishing schemes.

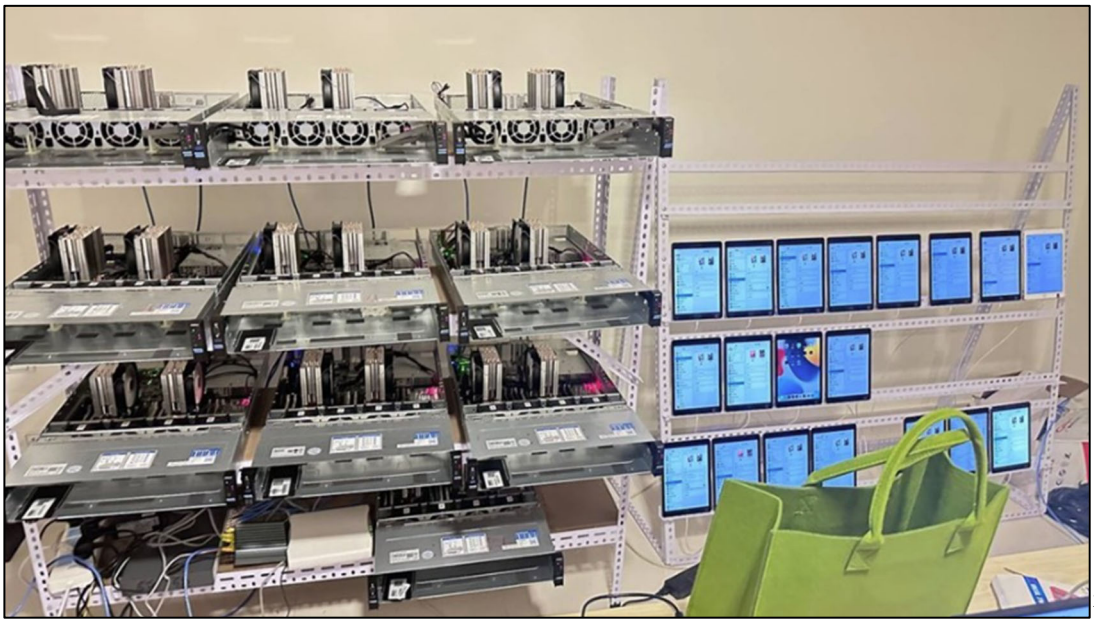
64. Another member of the Data Broker Group is user @xiaoyi990618, whose Telegram biography indicates that the user offers other members of the Enterprise products to facilitate phishing campaigns, including contact information for potential victims, the ability to

send bulk text messages to various devices, and point-of-sale machines allowing users to use stolen financial information to send money to themselves.

65. **The Spammer Group:** Members of the Spammer Group provide the tools to send fraudulent text messages in volume.

66. Large-scale smishing schemes require infrastructure to facilitate sending mass text messages. To send thousands of text messages simultaneously, the Enterprise needs banks of smartphones, SIM cards, modems, and services to support the data it demands. The Spammer Group provides these capabilities to other members of the Enterprise. For example, an individual, group of individuals, or entity acting under the username @x667788x helps send the messages necessary to contact victims of SMS scams—which often requires operating hundreds of cell phones at once.

67. Members of the Spammer Group shared the following pictures of their phishing "farms" on the Enterprise's Telegram channels, illustrating their operations:

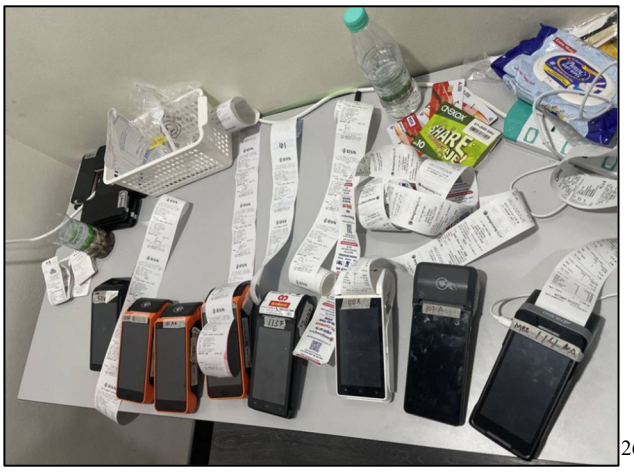
 [24]

[24] Erlend Leiknes & Harrison Sand, *Exposing Darcula: a rare look behind the scenes of a global Phishing-as-a-Service operation*, Mnemonic (May 4, 2025), https://tinyurl.com/537tm5bs.

 [25]

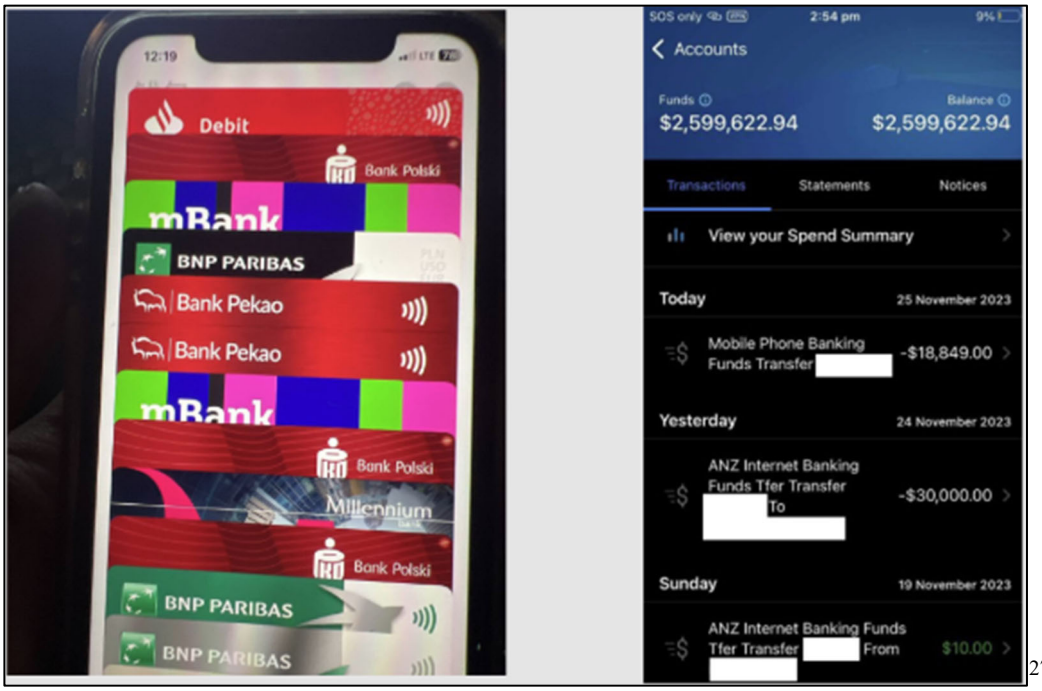
68. **The Theft Group:** Members of the Theft Group help to monetize stolen information.

69. These individuals or entities help steal money, social security information, and more once other members of the Enterprise acquire phished credentials from victims. For example, members of the Theft Group shared photos of payment terminals used to make purchases with stolen cards in the Administrative Group's Telegram channels, as shown below.

 [26]

[25] *Id.*
[26] *Id.*

70. With victims' credentials, the Theft Group can also access bank accounts, email accounts, brokerage accounts, and other sensitive accounts. These actors load stolen payment cards to digital wallets—like Google Wallet—and then resell phones containing the digital wallets that have stolen card information, which can be used to make purchases or launder money. Below are photos of digital wallets loaded with stolen credit cards and records of fraudulent transactions that Enterprise members shared in the Telegram channels.



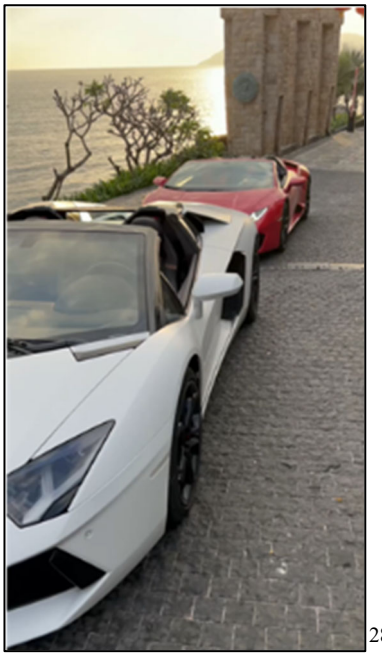
[27]

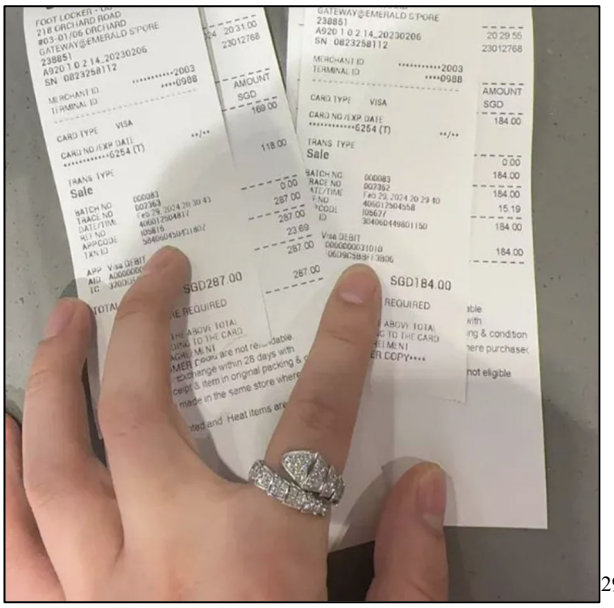
71. These groups coordinate with each other to recruit and train new members of the Enterprise, generate phishing strategies and tactics, select phishing targets, and coordinate phishing attacks. The Developer Group created the software and the Administrative Group markets it to recruit new members to the Enterprise. The Administrative Group also relays information about software updates to other members of the Enterprise and relays information from Enterprise members regarding software issues back to the Developer Group. Through the Administrative

[27] *Id.*

Group's Telegram channels, members of the Enterprise can plan phishing attacks and connect with the Data Broker Group and Spammer Group to utilize these groups' respective expertise and tools to execute attacks. Once the Enterprise has victim information in hand, the Theft Group monetizes, sells, or uses that information and helps to launder ill-gotten funds.

72. Working together, members of the Enterprise have amassed a significant amount of wealth and live a life of luxury funded by their victims. Members have posted about their success with the phishing schemes on social media, including on the Enterprise's Telegram channels:

 [28]

 [29]

73. Some members of the Darcula Enterprise have been described in investigative reporting published online. To avoid further detection, the Darcula Enterprise appears to have reduced its visible online presence for now, shuttering its Telegram channels and curtailing its efforts to expand. But Magic Cat's infrastructure remains intact and the Darcula Enterprise could resume its activities at any moment.

---

[28] *Id.*

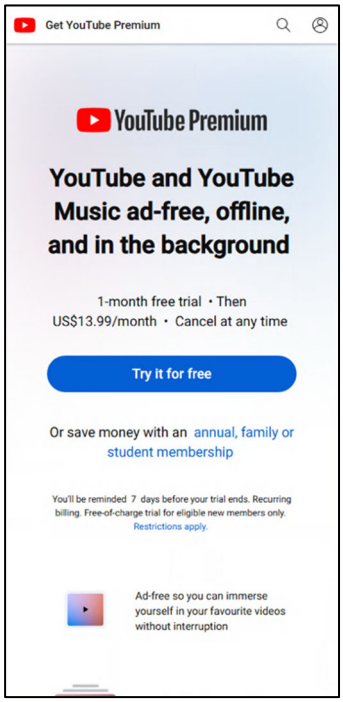
[29] Martin Gundersen, et al., *Inside the Scam Network*, NRK (May 4, 2025), https://tinyurl.com/5n6cp2jd.

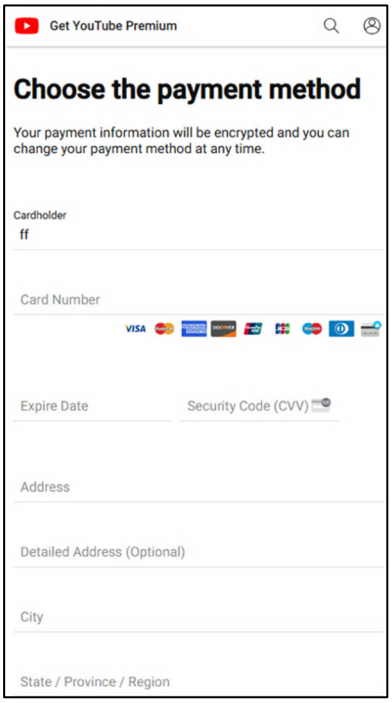
Fraudulent Schemes Executed by the Darcula Enterprise

74. Using Magic Cat, the Darcula Enterprise has been able to execute an astonishing number of phishing schemes. At its peak, researchers estimated that the Enterprise originated ***70 to 80% of all smishing messages***. Although Magic Cat includes templates for hundreds of fraudulent websites, several of the most well-known and commonly used smishing schemes include the YouTube Scheme, the Delivery Scheme, and the Toll Scheme.

75. **The YouTube Scheme:** The Darcula Enterprise has targeted Google by creating a template designed to spoof the YouTube Premium enrollment page.

76. In this scheme, an Enterprise member may use a template included with Magic Cat V2 to create a fraudulent version of the YouTube Premium webpage. The template includes both a fraudulent homepage and a page where "new users" are directed to provide their credit card information, purportedly to sign up for a one-month free trial to YouTube Premium. When a victim provides their financial information, however, they do not gain access to YouTube Premium; instead, an Enterprise member steals their financial information.

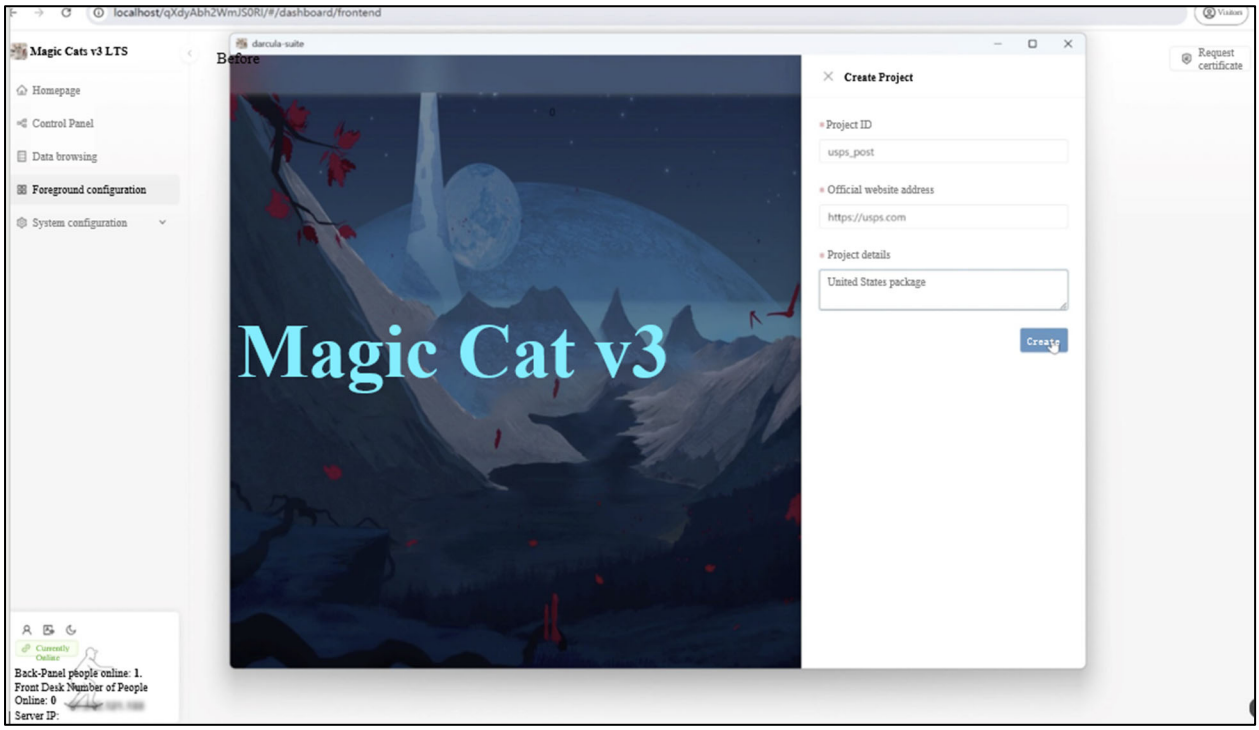




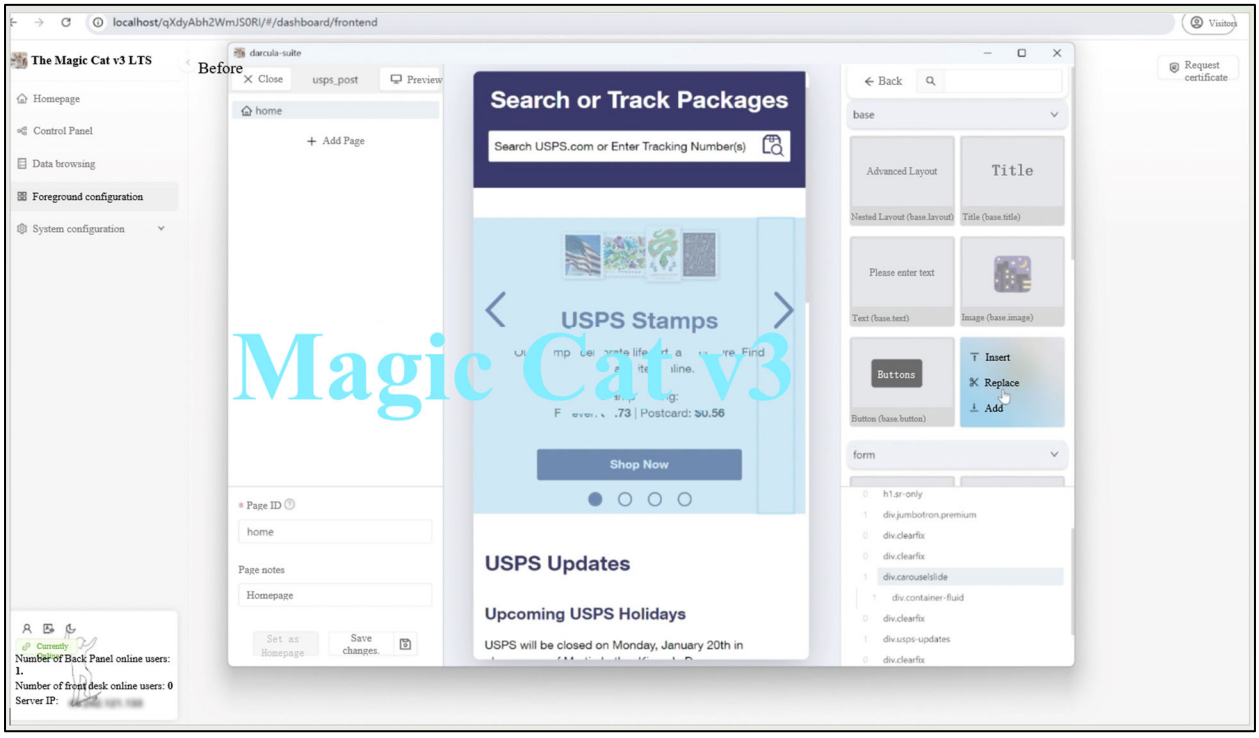
77. Members of the Enterprise collaborate to execute the attacks. For example, the Data Broker Group provides the Spammer Group with potential victims' phone numbers, and the Spammer Group in turn sends SMS or RCS messages in bulk to the phone numbers with links to the fraudulent webpage purporting to advertise a free trial to YouTube Premium. And once Enterprise members acquire victims' financial information, the Theft Group then provides opportunities to monetize the stolen personal and financial information, including by selling that information to other cybercriminals.

78. **Delivery Scheme:** The Darcula Enterprise's spoof of the USPS and other parcel delivery services is among the most common smishing attacks in operation.

79. To execute a delivery scheme using Magic Cat V3, members of the Enterprise first log in to a Magic Cat account and provide the URL that they would like to spoof, for example, https://usps.com:



80. Magic Cat sources images, text, and the website's design from the real USPS website, and creates a spoofed website that members of the Enterprise can edit and customize. An example is pictured below:



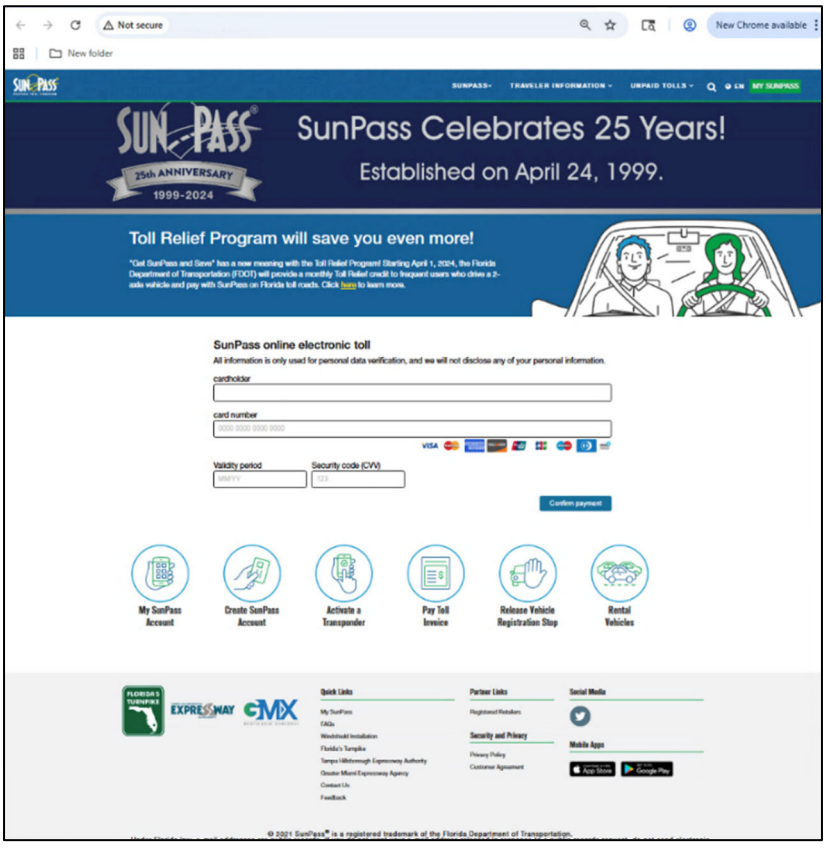
81. Once the spoofed website is customized, Enterprise members carrying out the attack can coordinate using the Enterprise's Telegram channels. For example, if Enterprise members are unable to transmit texts in bulk, they can retain members of the Spammer Group, who will send mass text messages for a fee.

82. The Darcula Enterprise then sends a carefully crafted text message to the targets, purporting to be USPS. Those texts are designed to convey a sense of urgency: in one example, they may purport to alert the target to a missed package delivery and include a link where the target can reschedule the delivery. If a target clicks the link, they are directed to a fake USPS website that requires payment of a small redelivery fee.

83. As the targets enter their personal financial details, the Magic Cat interface alerts the Enterprise through text messages or Telegram messages and simultaneously logs the target's keystrokes. The target need not actually submit the payment for the Enterprise to obtain the target's payment information. The Enterprise can then access that information on their Magic Cat account, where the software collects and organizes victims' stolen data, making it easier for the Enterprise to use that stolen data. Using the @darcula_channel on Telegram, the Enterprise posted a video tutorial that trains other Enterprise members to use Magic Cat to perpetrate the USPS scam.

84. **Toll Scheme:** Another common scam involves text messages purporting to pursue unpaid tolls.

85. Magic Cat includes hundreds of templates for fake websites, including many that replicate toll collection agencies. For example, Magic Cat offers a fake version of the Florida SunPass toll collection agency, pictured below.



86. In Magic Cat V3, Enterprise members can also simply input the URL for the SunPass website to create a fraudulent version of the website's most recent iteration. The fraudulent version of the website replaces the website page designed to collect payments with code that funnels credit card information directly to the Enterprise member who controls the page.

87. In this scheme, Enterprise members again coordinate to execute the attack. For example, once an Enterprise member creates a fraudulent website (using one of the fake toll collection templates available on Magic Cat V2 or V3, or creating a website for any toll agency using Magic Cat's AI functionality on V3), the Data Broker Group can provide the Spammer Group with potential victims' phone numbers, and the Spammer Group in turn sends SMS or RCS messages in bulk to phone numbers using phone banks, SIM banks, and other tools they possess.

88. The targets then receive a text message purporting to be a notice of a past-due toll invoice or ticket with a link to the fraudulent website. Like the delivery scam, the toll scam requests that targets input personal financial information, such as their credit card number, to pay the purported past-due toll.

89. The Theft Group then provides opportunities to monetize the personal and financial information stolen by selling that information to other cybercriminals.

Harm to Google, its Users, and the Public

90. The Darcula Enterprise causes significant harm to its victims by stealing their information and money. In the words of one Darcula smishing scam victim, "it's really all of us that pays for it[.] … I get irritated and angry. They have no honor or pride in life when they are stealing money that others have worked hard for. It is a disgrace to humanity."[30]

[30] Martin Gundersen, *The Hunt for Darcula*, NRK (May 8, 2025), https://tinyurl.com/42bj5esj.

91. The scope and impact of the Darcula Enterprise using the Magic Cat software is enormous. A recent cybersecurity investigation into the Darcula Enterprise revealed that, at its height, it included over 600 cybercriminals, each working to execute its fraudulent smishing schemes by sending tens of thousands of text messages to intended victims every day.[31] Since March 2024, the Darcula Enterprise has disseminated approximately 90,000 phishing websites.[32] In a period of just seven months, the Enterprise stole nearly 900,000 credit cards globally, with nearly 40,000 credit cards stolen from victims in the United States alone during that period.[33]

92. For almost three years, between 2023 and May 2025, the Darcula Enterprise operated openly through largely public online channels, apparently confident that its criminal enterprise was not vulnerable to disruption. But in May 2025, a team of journalists and cybersecurity experts published an in-depth report about the Darcula Enterprise, which caused the Enterprise to shutter many of its public communication channels and significantly reduce its public operations.

93. But Google's investigation has shown that the Enterprise is still active and working from the shadows, albeit on a smaller scale, creating and disseminating new phishing domains daily through Magic Cat.

94. In just a 25-day period between September 11 and October 5, 2025, for example, over 4,750 Google Messages users, including users in the United States, reported to Google

[31] Martin Gundersen, *Inside the Scam Network*, NRK (May 4, 2025), https://tinyurl.com/5n6cp2jd.
[32] *See* Harry Everett, *AI-Enabled Darcula-Suite Makes Phishing Kits More Accessible, Easier to Deploy*, Netcraft.com (Apr. 24, 2025), https://tinyurl.com/ms5a9m69.
[33] Davey Winder, *884,000 Credit Cards Stolen With 13 Million Clicks By A Magic Cat*, Forbes (May 6, 2025), https://tinyurl.com/3rudpxd6; Alexander Nabert et al., *The Chinese Scammers Behind the Fake DHL Messages*, BR24 (May 4, 2025), https://tinyurl.com/ymaj9zcs.

fraudulent phishing messages they received attempting to lure them into clicking on domains with spoofed websites created through Magic Cat.

95. For example, some messages read:

a. "Delivery is suspended because your delivery note does not include a house number. Please update as soon as possible";

b. "Your order details are incomplete or incorrect. Please review and update the information to avoid shipping delays"; and

c. "We've detected multiple attempts to log into your account. If this was not you, please block it."

96. In each instance, these messages are followed by links to phishing websites created by the Enterprise with Magic Cat.

97. Google's investigation into these thousands of fraudulent phishing messages to Google users identified hundreds of different phishing domains with spoofed websites that the Darcula Enterprise created and disseminated through Magic Cat.

98. Magic Cat's AI capabilities allow the software to be scaled to unprecedented levels. Any website can be replicated nearly perfectly, down to the brand logos of other products like Google Play or YouTube.

99. The Darcula Enterprise also harms Google by damaging customer trust and goodwill and forcing Google to devote significant time and resources to remediation efforts.

100. Specifically, the Darcula Enterprise targets Google Messages users by transmitting phishing messages through the RCS messaging protocol that Google has adopted in Google Messages.

101. The Enterprise has also prominently featured Google's branding and logos, specifically:

a. in Magic Cat tutorial videos used to instruct Enterprise members how to generate spoofed websites for use in their phishing schemes;

b. in a template spoofing YouTube Premium, specifically targeting Google's customers and impersonating Google itself through attacks using this template; and

c. in spoofed website templates featuring Google's branding or logos on the sign-in screens.

102. The Enterprise's template spoofing the Florida SunPass's website features the Google Play logo, telling targets that they can download the spoofed brand's app in the Google Play store. Multiple other Magic Cat-spoofed websites include the Google Play and YouTube logos (along with logos of prominent social media sites), mimicking a common feature of real websites to again create a veneer of legitimacy.

103. Victims may view the presence of a Google or YouTube logo as an indicator that the website is safe or legitimate. The Enterprise is thus exploiting the Google branding—and the goodwill associated with it—to convince victims to turn over their sensitive personal and financial information.

104. The exploitation of Google's product, branding, and logos harms Google's public image and may encourage customers to move away from using Google's products and services.

105. The use of these logos violates Google's Rules for Proper Usage of its trademarks and brand features, which bar, among other things, "display[ing] a Google Brand Feature on a site that violates any law or regulation," "display[ing] a Google Brand Feature in any manner that implies a relationship or affiliation with … Google," or "display[ing] a Google Brand Feature in a

manner that is … misleading[] [or] infringing."[34] There are further requirements for the use of certain Google logos and icons. For example, Google's brand team must "review[] and fully approve[]" any use of the Google Play Mark.[35]

106. The Enterprise also uses Gmail accounts to distribute phishing messages to potential victims using Apple devices through iMessages linked to these Gmail accounts. And the Darcula Enterprise frequently distributes these phishing messages to potential victims using Android devices through Google Messages (through RCS).

107. This use of Google products violates Google's Terms of Service, which require account holders to agree that they will not be "accessing or using [Google] services in fraudulent or deceptive ways, such as … phishing" or "creating fake accounts."[36] The Enterprise facilitates illegal activities on Google's platforms and, therefore, causes damage to Google's customer relationships and reputation. Google actively investigates and terminates accounts supporting such activities as soon as possible.

108. Google has invested significant resources to combat Magic Cat, the Enterprise, and other cybersecurity threats. Google has spent thousands of dollars and over 150 hours investigating and remediating the Enterprise's activities, including engaging teams around the world. And Google will have to continue these efforts as long as the Darcula Enterprise continues to develop, distribute, and deploy Magic Cat.

[34] Google, *Rules for Proper Usage*, Brand Res. Ctr., https://tinyurl.com/24dvmced (last visited Nov. 6, 2025).
[35] Google, *Google Play Legal Requirements*, Partner Mktg. Hub, https://tinyurl.com/2yz2mscd (last visited Nov. 6, 2025).
[36] Google, Terms of Service, https://tinyurl.com/ynm67nz3 (last visited Dec. 14, 2025).

CLAIMS FOR RELIEF

COUNT I
Violations of the Racketeer Influenced and Corrupt Organizations Act
18 U.S.C. § 1962(c)–(d)

109. Google incorporates by reference the foregoing paragraphs (¶¶ 1–108) of the Complaint as if set forth in full.

110. At all relevant times, Google is and has been a "person" within the meaning of 18 U.S.C. § 1961(3).

111. At all relevant times, Google is and has been a "person injured in his business or property by reason of a violation of" RICO within the meaning of 18 U.S.C. § 1964(c).

112. At all relevant times, each Defendant is and has been a person within the meaning of 18 U.S.C. §§ 1961(3) and 1962(c).

113. Under 18 U.S.C. § 1964(c), Google is entitled to recover treble damages plus costs and attorneys' fees from the Defendants.

The RICO Enterprise

114. Defendants are a group of persons associated together in fact for the common purpose of carrying out an ongoing criminal enterprise, as described in the foregoing paragraphs of this Complaint. Specifically, Defendants, as members of the Darcula Enterprise, have worked together over time to create, control, and use Magic Cat to execute numerous criminal schemes that harm and threaten to continue to harm Google, its users, and the general public.

115. As described *supra* at paragraphs 47 through 73, Defendants have organized themselves into a network of cybercriminals operating in the United States and overseas, targeting victims in the United States. Over time, they have adapted their operations and schemes, enlisted new threat actors in their operation, and expanded the scope and nature of their activities.

116. Utilizing Magic Cat to execute a wide variety of phishing schemes, Defendants act with the common purpose of enriching themselves and fraudulently obtaining sensitive personal and financial information. Specifically, Defendants have collaborated to establish, grow, manage, and deploy Magic Cat. To enrich themselves, members of the Enterprise all take part in directing the aspects of its phishing schemes: some develop and improve the Magic Cat software; others manage the Telegram channels where Magic Cat is marketed and sold and the Enterprise discusses their schemes; others supply lists of potential victims' contact information; still others share strategies for sending bulk text messages and identifying victims; and others help steal money, social security information, and more once other members of the Enterprise acquire phished credentials.

117. Defendants constitute an association-in-fact enterprise within the meaning of 18 U.S.C. §§ 1961(4) and 1962(c). The existence of this association-in-fact is evidenced by Defendants' membership and communication in the Enterprise's Telegram channels, common use of Magic Cat, coordination in executing phishing attacks, and the commercialization of the attacks, which indicates that Defendants function like a black-market business enterprise. *Supra* ¶¶ 47–89.

118. At all relevant times, the Darcula Enterprise has been engaged in these activities, and its activities have affected interstate and foreign commerce within the meaning of 18 U.S.C. § 1962(c).

Pattern of Racketeering Activity and RICO Predicate Acts

119. At all relevant times, Defendants have conducted or participated in, directly or indirectly, the conduct, management, and/or operation of the Darcula Enterprise through a pattern of racketeering activity within the meaning of 18 U.S.C. § 1961(5) and in violation of 18 U.S.C. § 1962(c), with such conduct and activities affecting interstate and foreign commerce.

120. Defendants have directly or indirectly engaged in an unlawful pattern of racketeering activity involving thousands of RICO predicate offenses, including wire fraud in violation of 18 U.S.C. § 1343. This statutory violation is incorporated as a RICO predicate act under 18 U.S.C. § 1961(1). These activities have affected and continue to affect interstate or foreign commerce.

121. Google has been injured in its business and property by reason of Defendants' violations of 18 U.S.C. § 1962(c), as described herein, including through Defendants' smishing schemes and by having to devote substantial financial resources to combat Defendants' criminal schemes. These injuries are a direct, proximate, and reasonably foreseeable result of these violations, and Google will continue to be harmed absent the relief requested here.

Wire Fraud Predicate Offenses (18 U.S.C. § 1343)

122. Defendants, with intent to defraud and obtain money or property by means of false or fraudulent pretenses, commit wire fraud in violation of 18 U.S.C. § 1343 by transmitting or causing to be transmitted, by means of wire communication in interstate or foreign commerce, writings, signs, and signals for the purpose of executing fraudulent schemes. Defendants have violated and continue to violate the wire fraud statute.

123. Defendants commit wire fraud in violation of 18 U.S.C. § 1343 each time that they send a fraudulent phishing message to an individual in the United States for the purposes of defrauding that individual into submitting sensitive personal and/or financial information through misrepresentation and deception in order to steal that individual's money or property. For example, the Darcula Enterprise misleads victims by using the names and websites of legitimate entities, such as USPS, to turn over that information, as described *supra* ¶¶ 78–80.

124. Between September and December 2025, over 5,000 Google Messages users reported to Google fraudulent messages they received from Defendants to perpetrate phishing schemes to steal money from these targets. For example:

a. On September 25, 2025, a U.S.-based Google Messages user reported receiving a phishing message from Defendants that stated, "We've detected multiple attempts to log into your account. If this was not you, please block it," followed by a link to a website domain created through Magic Cat to spoof the website of a U.S.-based financial institution.

b. On October 1, 2025, two different U.S.-based Google Messages users reported receiving a message from Defendants with text identical to the message quoted above, each followed by a link to a different website domain created through Magic Cat to spoof the website of the same U.S.-based financial institution.

c. On October 5, 2025, another U.S.-based Google Messages user reported receiving a message from Defendants with text identical to the message quoted above, again with a link to another website domain created through Magic Cat to spoof the website of the same U.S.-based financial institution.

d. On November 19, 2025, a U.S.-based Google Messages user reported receiving a phishing message from Defendants that stated, "Your updated 401(k) balance is ready to view. Please sign in for your most recent information," followed by a link to a website domain created through Magic Cat to spoof the website of a U.S.-based financial institution.

e. On November 27, 2025, another U.S.-based Google Messages user reported receiving a message from Defendants with text identical to the message quoted

above, again with a link to a website domain created through Magic Cat to spoof the website of the same U.S.-based financial institution.

125. Defendants sent each of these phishing messages through interstate or foreign wires with the intent to defraud the Google Messages user into entering his or her personal and financial information for the purpose of stealing money from his or her account.

126. Google has suffered direct injury to its business or property as a result of these wire fraud predicate offenses, including the substantial sums of money it has invested to investigate, remediate, and prevent these acts from being perpetrated on its customers and through its services.

Conspiracy to Violate RICO

127. Google incorporates the foregoing paragraphs (¶¶ 1–126) of the Complaint as if set forth in full.

128. Defendants have not undertaken the practices described herein in isolation, but rather as part of a common scheme. In violation of 18 U.S.C. § 1962(d), each Defendant unlawfully, knowingly, and willfully agreed and conspired together and with others to violate 18 U.S.C. § 1962(c) as described above, in violation of 18 U.S.C. § 1962(d).

129. Defendants knew that they were engaged in a conspiracy to commit multiple predicate offenses, and that the predicate offenses were part of a pattern of racketeering activity. Defendants' participation in the conspiracy and agreement to commit those offenses were necessary to facilitate this pattern of racketeering activity. This conduct constitutes a conspiracy to violate 18 U.S.C. § 1962(c), in violation of 18 U.S.C. § 1962(d).

130. Defendants agreed to direct or participate in, directly or indirectly, the conduct, management, or operation of the Darcula Enterprise through a pattern of racketeering activity in violation of 18 U.S.C. § 1962(c). Each Defendant knew about and agreed to facilitate the Darcula Enterprise's affairs. The purpose of the conspiracy was to commit a pattern of racketeering activity

in the conduct of the affairs of the Darcula scheme, including the acts of racketeering set forth above, including the sale and use of Magic Cat to commit crimes, enriching the Enterprise.

131. Google has been and continues to be directly injured by Defendants' conduct. But for the alleged pattern of racketeering activity, Google would not have incurred damages.

132. Google seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

133. As a direct result of Defendants' actions, Google has suffered and continues to suffer irreparable harm for which there is not an adequate remedy at law and which will continue unless Defendants' actions are enjoined.

COUNT II
Violations of the Lanham Act
15 U.S.C. §§ 1114(1), 1125(a)(1)(A), 1125(a)(1)(B)

134. Google incorporates the foregoing paragraphs (¶¶ 1–133) of the Complaint as if set forth in full.

135. Google has devoted substantial efforts and resources, both in the United States and internationally, to promoting its services using its Marks.

136. Google's Marks reflect the valuable reputation and goodwill that Google has earned in the marketplace for its high-quality and innovative services.

137. Defendants and/or their agents used the Marks to legitimize their fraudulent websites which tricked victims into turning over sensitive personal and/or financial information to Defendants.

138. Defendants used Google's Marks in connection with the advertising of services in commerce in a manner that is likely to cause confusion, to cause mistake, or to deceive.

Infringement of Federally Registered Marks
15 U.S.C. § 1114(1)

139. Defendants' and/or their agents' use of Google's Marks in commerce has caused and/or is likely to continue to cause confusion with Google's federally registered Marks, in violation of 15 U.S.C. § 1114(1). The use by Defendants and/or their agents of the Marks has caused and/or is likely to continue to cause confusion and mistake; has deceived and/or is likely to continue to deceive potential customers and the relevant purchasing public as to the source, origin, or sponsorship of Defendants' services; and has deceived and/or is likely to continue to deceive the public into believing that those services originate from, are associated with, or are otherwise authorized by Google, to the damage and detriment of Google's reputation, goodwill, and sales.

140. Google has no adequate remedy at law, and, if Defendants' actions are not enjoined, Google will continue to suffer irreparable harm to its reputation and the goodwill of its well-known Marks. 15 U.S.C. § 1116(a).

141. Further, Defendants have caused damage to Google, and they have profited from their unlawful actions in an amount not known to Google.

Unfair Competition and False Designation of Origin
15 U.S.C. § 1125(a)(1)(A)

142. Defendants' and/ or their agents' use of the Google Marks in commerce has caused and/or is likely to cause confusion in violation of 15 U.S.C. § 1125(a)(1)(A). Defendants' and/or their agents' use of the Google Marks and/or images associated with Google has caused and/or is likely to cause confusion and mistake; has deceived and/or is likely to continue to deceive potential customers and the relevant purchasing public as to the source, origin, or sponsorship of Defendants' services; and has deceived and/or is likely to continue to deceive the public into

believing that those services originate from, are associated with, or are otherwise authorized by Google, to the damage and detriment of Google's reputation, goodwill, and sales.

143. Google has no adequate remedy at law, and, if Defendants' actions are not enjoined, Google will continue to suffer irreparable harm to its reputation and the goodwill of its well-known Marks. 15 U.S.C. § 1116(a).

144. Further, Defendants have caused damage to Google, and they have profited from their unlawful actions in an amount not known to Google.

False Advertising
15 U.S.C. § 1125(a)(1)(B)

145. Defendants' and/or their agents' false, deceptive, and misleading advertising in interstate commerce violates Section 43(a) of the Lanham Act, 15 U.S.C. § 1125(a)(1)(B).

146. Defendants' and/or their agents' advertising claims regarding alleged services offered by Defendants, including featuring Google's Marks, are false, deceptive, and/or misleading.

147. Defendants' and/or their agents' false, deceptive, and misleading claims were included in their commercial advertising and/or promotional materials.

148. Defendants and/or their agents have distributed their false, deceptive, and misleading advertising claims in interstate commerce.

149. Defendants' and/or their agents' false, deceptive, and misleading advertising claims have the capacity to deceive end users and are material to end users' decisions to engage with Defendants.

150. Google has been injured as a result of this false, deceptive, and misleading advertising.

151. Google will continue to be irreparably injured unless and until Defendants' conduct is preliminarily, and thereafter, permanently enjoined by this Court, and Google has no adequate remedy at law. 15 U.S.C. § 1116(a).

152. As a direct and proximate result of Defendants' false, deceptive, and misleading advertising, Google has suffered harm and damages in an amount to be determined by the trier of fact.

153. Defendants and/or their agents have engaged in intentional and willful violation of the Lanham Act entitling Google to enhanced damages and attorneys' fees and costs.

COUNT III
Computer Fraud and Abuse Act Violation
18 U.S.C. § 1030(a)(6)

154. Google incorporates the foregoing paragraphs (¶¶ 1–153) of the Complaint as if set forth in full.

155. Defendants have violated and continue to violate the CFAA, 18 U.S.C. § 1030(a)(6), resulting in loss to one or more persons during a one-year period amounting in the aggregate to at least $5,000 in value.

156. Defendants knowingly and with intent to defraud trafficked passwords or similar information through which a computer may be accessed without authorization.

157. Defendants collected usernames, credit card information, authorization codes, and other similar information from device users without the users' authorization and transferred users' usernames, credit card information, authorization codes, and other similar information to digital wallets and/or other individuals, including individuals paying for the information.

158. Defendants' conduct involved interstate and/or foreign communications.

159. Defendants' conduct has caused a loss to one or more persons, including Google, during a one-year period aggregating at least $5,000. 18 U.S.C. § 1030(c)(4)(A)(i)(I).

160. Specifically, Google has suffered loss as a result of Defendants' CFAA violations in the form of reasonable costs of responding to Defendants' scheme, including conducting damage assessments. *See* 18 U.S.C. § 1030(e)(11). Over the period from January 2025 to December 2025, those losses have exceeded $5,000.

161. Google seeks injunctive relief and compensatory damages in an amount to be proven at trial. *See* 18 U.S.C. § 1030(g).

162. As a direct result of Defendants' actions, Google has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

PRAYER FOR RELIEF

WHEREFORE, Google prays for judgment as set forth below:

A. Judgment in favor of Google and against Defendants;

B. A declaration that Defendants have engaged in acts or practices that violate the RICO, Lanham Act, and CFAA statutes;

C. A declaration that Defendants' conduct has been willful and that Defendants have acted with fraud, malice, and oppression;

D. A temporary restraining order and preliminary and permanent injunctions enjoining Defendants and their officers, directors, principals, agents, servants, employees, successors, and assigns, and all persons and entities in active concert or participation with them, from engaging in any of the activity complained of herein or from causing any of the injury complained of herein and from assisting, aiding, or abetting any other person or business entity in engaging in or performing any of

the activity complained of herein or from causing any of the injury complained of herein;

E. Award of appropriate equitable relief available under applicable statutes and law, including injunctive relief;

F. Judgment awarding Google actual and/or statutory damages from Defendants adequate to compensate Google for Defendants' activity complained of herein and for any injury complained of herein, including but not limited to interest and costs, in an amount to be proven at trial;

G. Judgment awarding enhanced, exemplary, and special damages, in an amount to be proven at trial;

H. Judgment awarding attorneys' fees and costs; and

I. Such other relief that the Court deems just and reasonable.

Dated: December 17, 2025

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

Christine M. Carletta
Paul Weeks (*pro hac vice* to be submitted)
KING & SPALDING LLP
1700 Pennsylvania Avenue, NW, Suite 900
Washington, DC 20006-4707
Tel: (202) 737-0500
Fax: (202) 626-3737
ccarletta@kslaw.com
pweeks@kslaw.com

Sumon Dantiki (*pro hac vice* to be submitted)
BAKER MACKENZIE LLP
815 Connecticut Avenue, N.W.
Washington, DC 20006
Tel: (202) 452-7000
Fax: (202) 452-7074
sumon.dantiki@bakermckenzie.com

Counsel for Plaintiff Google LLC

Exhibit 2

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Southern District of New York

GOOGLE LLC,

Plaintiff(s)

v.

DOE 1 a/k/a YUCHENG CHANG and DOES 2–25,

Defendant(s)

Civil Action No. 1:25-cv-10440-JSR

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* DOE 1 a/k/a YUCHENG CHANG and DOES 2–25

See attached rider for additional service information, including email addresses known to be associated with Does.

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are: 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

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

Date: FEB 19 2026

Tammi M. Hellwig
CLERK OF COURT

Signature of Clerk or Deputy Clerk

Civil Action No. 1:25-cv-09421

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____

was received by me on *(date)* _____.

❒ I personally served the summons on the individual at *(place)* _____

_____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____

_____, a person of suitable age and discretion who resides there,

on *(date)* _____, and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____, who is

designated by law to accept service of process on behalf of *(name of organization)* _____

_____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify)*:

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____

Server's signature

_____

Printed name and title

_____

Server's address

Additional information regarding attempted service, etc:

***Google LLC v. DOE 1 a/k/a YUCHENG CHANG and DOES 2–25*, 1:25-cv-10440**

Google will serve Doe 1 a/k/a Yucheng Chang and Does 2–25, by publication through a publicly-available website, magiccatdarculaserviceofprocess.com, and by the email addresses obtained through domain registrars, as reflected below.

Email Addresses for Service of Process on Doe Defendants

feltonhamm@gmail.com
my4cheng@gmail.com
nasinacarina467@gmail.com
hsjuge1655@gmail.com
cartera@colegiodulcemaria.edu.co
grannisfarella@gmail.com
rafekgnt2851@hotmail.com
golombouska@gmail.com
xhgtbn@163.com
gabrieltristan6787@gmail.com
jiangya670@163.com
murazor4006@gmail.com
uejehrhtbbt@gmail.com
killer543809@gmail.com
yuemanceshi@gmail.com
halukiakilaqhalukiakila@gmail.com
summer96960606@gmail.com
deborahwiosk@aol.com
heimao00777@gmail.com
yvbgldwcoqiay@outlook.com
fabianarleen68025@hotmail.com
ettstryk@gmail.com
renvex00@gmail.com
king_lisaz85166@gmx.com
4748453@gmail.com
haqbarby@gmail.com
quintrusen@gmail.com
cjon55699@gmail.com
xudada123654@gmail.com
zhuzhu306706183@gmail.com
vslskie82320wkwk@gmail.com

EXHIBIT 3

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC, *Plaintiff,* v. DOE 1 a/k/a YUCHENG CHANG and DOES 2–25, *Defendants.*	Civil Action No.:

PLAINTIFF'S MOTION FOR AN *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

Plaintiff Google LLC ("Google" or "Plaintiff"), by and through undersigned counsel, hereby moves this Court to enter an *ex parte* temporary restraining order and an order to show cause against Defendants Doe 1 a/k/a Yucheng Chang and Does 2–25 in accordance with Federal Rule of Civil Procedure 65. The proposed order is necessary to prevent Google, its users, and the public from suffering further and irreparable harm because of Defendants' acts. The grounds for this motion and order are set forth in the accompanying memorandum of law.

Dated: December 17, 2025

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

Christine M. Carletta
Paul Weeks (*pro hac vice* to be submitted)
KING & SPALDING LLP
1700 Pennsylvania Avenue, NW, Suite 900
Washington, DC 20006-4707
Tel: (202) 737-0500
Fax: (202) 626-3737
ccarletta@kslaw.com
pweeks@kslaw.com

Sumon Dantiki (*pro hac vice* to be submitted)
BAKER MACKENZIE LLP
815 Connecticut Avenue, N.W.
Washington, DC 20006
Tel: (202) 452-7000
Fax: (202) 452-7074
sumon.dantiki@bakermckenzie.com

Counsel for Plaintiff Google LLC

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC, *Plaintiff,* v. DOE 1 a/k/a YUCHENG CHANG and DOES 2–25, *Defendants.*	Civil Action No.:

[PROPOSED] *EX PARTE* TEMPORARY RESTRAINING ORDER
AND ORDER TO SHOW CAUSE

Plaintiff Google LLC ("Google" or "Plaintiff") has filed a Complaint for injunctive and other relief to stop Defendants Doe 1 a/k/a Yucheng Chang and Does 2–25, a criminal enterprise (the "Darcula Enterprise" or the "Enterprise"), from using novel software to facilitate large-scale phishing attacks that have harmed over one million victims, including Google.

Google filed a Complaint alleging claims under (1) the Racketeer Influenced and Corrupt Organizations Act ("RICO"), 18 U.S.C. § 1962(c)–(d) (Count I); (2) the Lanham Act, 15 U.S.C. §§ 1114(1), 1125(a)(1)(A), 1125(a)(1)(B) (Count II); and (3) the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a)(6) (Count III). Google has moved under seal and *ex parte* for a temporary restraining order and an order to show cause why a preliminary injunction should not issue under Federal Rule of Civil Procedure 65 and 28 U.S.C. § 1651.

THE COURT HEREBY FINDS THAT:

1. This Court has federal-question jurisdiction over Google's claims under RICO, the Lanham Act, and the CFAA pursuant to 28 U.S.C. § 1331.

2. This Court has personal jurisdiction over Defendants because:

a. Defendants have intentionally targeted and harmed Google, a company based in the United States. Defendants also have engaged in intentional, wrongful, illegal, and/or tortious acts, the effects of which Defendants intended to and knew would be felt in the United States and New York. Google does business in New York and has done business in New York for many years, including in this District.

b. Defendants have affirmatively directed actions at the United States, including this District, and Defendants attempted to phish and have successfully phished personal and financial information from victims within this District and New York State.

c. Defendants have used Google's trademarks as part of fake websites used to solicit victims' personal and financial information within this District and New York State, and have directed multiple forms of electronic communication to user devices in this District and New York State.

3. Venue is proper in this judicial district under 28 U.S.C. § 1391(c)(3) because Defendants are not residents of the United States and may be sued in any judicial district. Venue is also proper in this judicial district under 28 U.S.C. § 1391(b)(2) and 18 U.S.C. § 1965(a) because a substantial part of the events or omissions giving rise to Google's claims occurred in this judicial district, because a substantial part of the harm caused by Defendants has occurred in this judicial district, and because Defendants transact their affairs in this judicial district. Moreover, Defendants are subject to personal jurisdiction in this judicial district, and no other venue appears to be more appropriate.

4. The Complaint pleads facts with the specificity required by the Federal Rules of Civil Procedure and states claims against Defendants for violations of (1) RICO, 18 U.S.C.

§ 1962(c)–(d) (Count I); (2) the Lanham Act, 15 U.S.C. §§ 1114(1), 1125(a)(1)(A), 1125(a)(1)(B) (Count II); and (3) the CFAA, 18 U.S.C. § 1030(a)(6) (Count III).

Temporary Restraining Order Factors

5. The Court finds that Google has established each of the factors required for a temporary restraining order: (1) specific facts in declarations show that Google is likely to suffer immediate, irreparable harm before Defendants can be heard; (2) Google is likely to succeed on the merits and/or has established a substantial question as to the merits; (3) the balance of hardships tips in Google's favor; and (4) a temporary restraining order serves the public interest. *Citigroup Global Mkts., Inc. v. VCG Special Opportunities Master Fund Ltd.*, 598 F.3d 30, 34–35 (2d Cir. 2010); Fed. R. Civ. P. 65(b)(l)(A).

Irreparable Harm

6. Google has established by specific facts that in the absence of a temporary restraining order, it will suffer immediate, irreparable harm before Defendants can be heard in opposition. Defendants—through their operation of the Darcula Enterprise to participate in and carry out numerous criminal phishing scams (the "Darcula Schemes")—have threatened the security of the Internet and are causing ongoing and irreparable harm to Google and the public by using phishing attacks to steal personal and financial information, defrauding unsuspecting targets, impairing Google's reputation and goodwill, and causing Google (and numerous others) unrecoverable financial losses. Until the Darcula Schemes are disrupted, the Enterprise will continue to profit from its unlawful activities at the expense of Google and members of the public.

7. Defendants' conduct is injuring Google's goodwill and damaging its reputation by falsely associating Google with fraud perpetrated by the Darcula Enterprise, and injuries to goodwill and reputation constitute irreparable harm. Google has suffered and continues to suffer

economic losses from the Darcula Schemes because Google has expended (and continues to expend) substantial financial resources into developing strong brand recognition associated with its name, logos, and products, and investigating and combat Darcula Schemes and to identify measures necessary to remediate the harms caused by the Darcula Schemes. These injuries constitute irreparable harm, including because Google has shown a likelihood that Defendants would take steps to avoid complying with any judgment.

Likelihood of Success on the Merits

8. Google has demonstrated that its Complaint presents a substantial question as to each of its claims and that it is likely to succeed on the merits of its claims. *See Sterling v. Deutsche Bank Nat'l Tr. Co. as Trs. for Femit Tr. 2006-FF6*, 368 F. Supp. 3d 723, 727 (S.D.N.Y. 2019).

9. *The Lanham Act*. Google has shown a likelihood of success on the merits of its claims that Defendants violated and continue to violate the Lanham Act. Section 1114 of the Lanham Act prohibits infringement of a registered trademark or service mark. Infringement occurs when a valid, protectable mark is used in commerce and is likely to cause confusion, to cause mistake, or to deceive. 15 U.S.C. § 1114(1); *Virgin Enters. Ltd. v. Nawab*, 335 F.3d 141, 146 (2d Cir. 2003). Defendants violated this provision by exploiting Google's trustworthy, well-known, valid, protectable, and registered Marks on their spoofed websites to deceive consumers. Section 1125(a) prohibits false "designations of origin" that are likely to cause confusion as to the sponsorship 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, *Victorinox AG v. B & F System, Inc.*, 114 F. Supp. 3d 132, 139 (S.D.N.Y. 2015), so Google's section 1125(a)(1)(A) claim is 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) have caused injury to the plaintiff. *Church & Dwight Co. v. SPD Swiss Precision Diagnostics, GmBH*, 843 F.3d 48, 65 (2d Cir. 2016). Google has demonstrated that Defendants deceive Internet users by using Google's Marks on their spoofed websites. Google has shown that the representations are literally false because they are not from or endorsed by Google and that the representations are material because the Defendants' schemes are only successful because their websites appear to be real. The messages bearing Google Marks are placed in interstate commerce on the Internet, and Google has demonstrated injury to its goodwill and through costs to combat the Darcula Schemes. Google is thus likely to succeed on its Lanham Act claims.

10. *RICO*. Google has shown a likelihood of success on the merits of its claim that Defendants have violated and continue to violate the RICO statute, and that Defendants engaged in a RICO conspiracy.

a. Google has shown that Defendants are active participants in the operation and management of the Darcula Enterprise, which uses Magic Cat 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.

b. Google has established that Defendants constitute an enterprise. Defendants are associated-in-fact and share a common purpose defrauding victims into disclosing sensitive personal information, including financial account details, and stealing their money. Darcula Enterprise members all take part in directing the aspects of the scheme: some develop the Magic Cat software, architecture, and user interface; others manage an online community that recruits new Enterprise members; others supply potential victims' contact information; others specialize in phishing

strategies; and still others steal information and money from victims after the Enterprise phishes their credentials. Defendants collaborate to establish, grow, and manage the Darcula Enterprise, and coordinate to execute sophisticated phishing schemes.

c. Google has established that Defendants have engaged in a pattern of racketeering activity. *See* 18 U.S.C. § 1961(1), (5); *id.* § 2332b(g)(5)(B). The predicate acts include violations of the federal wire fraud statute, 18 U.S.C. § 1343. Defendants have, with intent to defraud and obtain money or property by means of false or fraudulent pretenses, committed wire fraud and continue to commit wire fraud by transmitting signals in interstate or foreign commerce for the purpose of deceiving device owners into submitting sensitive personal or financial information through deception, in violation of 18 U.S.C. § 1343.

d. Google has suffered injury to its business or property as a result of these predicate offenses by devoting substantial financial resources to investigate and remediate Defendants' criminal schemes in order to protect its goodwill and reputation.

e. Google has demonstrated that Defendants have engaged in a RICO conspiracy. The links among the Defendants—such as use of the Magic Cat software, communication over dedicated Telegram channels, and the methods used to deploy phishing schemes using Magic Cat and other Enterprise-controlled resources—demonstrate that the Enterprise formed an agreement as part of a common scheme and conspiracy.

11. *CFAA*. Google has shown a likelihood of success on the merits of its claim that Defendants violated and continue to violate the CFAA. Google has demonstrated that Defendants

have—knowingly and with intent to defraud—trafficked in passwords or similar information through which a computer may be accessed without authorization in interstate commerce through Telegram channels and other online forums in violation of 18 U.S.C. § 1030(a)(6). Defendants transfer and sell phished account credentials and authorization codes to other members of the Enterprise and other cybercriminals. Defendants' actions have caused loss to one or more persons in excess of $5,000 in a one-year period. *See id*. §§ 1030(g), 1030(c)(4)(A)(i)(I), including loss to Google, *see id.* § 1030(e)(11); *see also Saunders Ventures, Inc. v. Salem*, 797 F. App'x 568, 572–73 (2d Cir. 2019).

Balance of Hardships

12. The equities also favor a temporary restraining order. The Darcula Enterprise is defrauding consumers and injuring Google and continues to victimize more people each day. No countervailing factors weigh against a temporary restraining order. There is no legitimate reason why Defendants should be permitted to continue to weaponize Google's branding to defraud the public and commit cybercrimes.

Public Interest

13. Google has shown that the public interest favors granting a temporary restraining order.

14. The Darcula Enterprise has defrauded over one million victims, while using their ill-gotten funds to support other criminal schemes. With each passing day, Defendants deceive new victims. Protection from malicious cyberattacks and other cybercrimes is strongly in the public interest.

15. The public interest is also served by enforcing statutes designed to protect the public, including RICO, the Lanham Act, and the CFAA.

Good Cause for *Ex Parte* Relief

16. As discussed above, Google has set forth facts demonstrating immediate and irreparable harm. There is good cause to believe that if Defendants are provided advance notice of Google's TRO application or this Order, they would dissipate the Darcula Enterprise's infrastructure and resources, allowing them to continue their misconduct, and they would destroy, move, hide, conceal, or otherwise make inaccessible to the Court evidence of their misconduct.

Good Cause for Alternative Service

17. The Court finds good cause exists to grant alternative service of the filings in this matter by email using any information available from web-hosting companies provided in connection with domain names used in the Darcula Schemes and/or any email addresses identified through Google's investigation; website publication; and/or other means because Google establishes that traditional service methods would be futile. Given the online nature of Defendants' conduct, online alternative service is most likely to give Defendants notice of the filings pertaining to this lawsuit.

TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

IT IS HEREBY ORDERED that Defendants, their officers, agents, servants, employees, attorneys, and all others in active concert or participation with them, and each of the foregoing, who receive actual notice of this Order by personal service or otherwise ("Restrained Parties"), are temporarily restrained and enjoined, from, anywhere in the world:

18. Using, linking to, transferring, selling, exercising control over, or otherwise owning any interest in or accessing Magic Cat or the Internet domains through which the Darcula Enterprise perpetrates its phishing schemes, set forth in **Appendix A** to the Naxo Declaration in

Support of Plaintiff's Motion for an *Ex Parte* Temporary Restraining Order and Order to Show Cause ("Appendix A");

19. Attacking and compromising the security of the computers and networks of Google's customers;

20. Intentionally accessing protected computers and computer networks of Google's customers without authorization;

21. Sending messages or advertisements with links to malicious websites;

22. Engaging in phishing schemes;

23. Stealing or selling credentials from victims of phishing schemes;

24. Monitoring the activities of Google or Google's customers or stealing information from them;

25. Impersonating Google, its systems, products, and services;

26. Creating websites that falsely indicate that they are associated with Google, YouTube, or any other Google product or affiliate, through use of Google's trademarks and/or other false and/or misleading representations;

27. Misappropriating that which rightfully belongs to Google, Google's customers and users, or in which Google has a proprietary interest;

28. Configuring, deploying, operating, or otherwise participating in or facilitating the Darcula Enterprise described in the moving papers, including but not limited to the Internet domain names listed in Appendix A and through any other component or element of Defendants' illegal infrastructure in any location, including infrastructure Defendants may attempt to rebuild;

29. Delivering malicious code designed to steal credentials;

30. Selling access to the accounts of Google's customers;

31. Offering, promoting, or selling victims' credit cards or other financial information to others for use;

32. Using, transferring, exercising control over, or accessing any accounts used in the transfer of money or electronic currency, including cryptocurrency, or in the processing of card-based transactions, as a means to further Defendants' unlawful schemes; and/or

33. Undertaking any similar activity that inflicts harm on Google, Google's customers, or the public.

34. Upon service as provided for in this Order, Defendants and other Restrained Parties shall be deemed to have actual notice of the issuance and terms of the Order, and any act by any of the Restrained Parties in violation of any of the terms of the Order may be considered and prosecuted as contempt of court.

35. The Clerk of the Court is to issue a summons to Defendant Doe 1 a/k/a Yucheng Chang and a summons to Defendants Does 2–25 for Google to serve on Defendants.

36. Service of this Order shall be effectuated on or before January 4, 2025.

IT IS FURTHER ORDERED that the Restrained Parties are temporarily restrained and enjoined from:

37. Using and infringing Google's trademarks, including but not limited to Plaintiff's Google mark (RN: 5365541), Google Play mark (RN: 5628029), and YouTube mark (RN: 87984068), and/or other trademarks, trade names, service marks, or Internet domain addresses or names containing or infringing such trademarks, trade names or service marks, as set forth in **Appendix B** to the Google Declaration in Support of Plaintiff's Motion for an *Ex Parte* Temporary Restraining Order and Order to Show Cause, which contains Google's trademarks, trade names, service marks, or Internet domain addresses or names containing or infringing such trademarks,

trade names or service marks, or other intellectual property infringed as a result of Defendants' activities;

38. Using in connection with Defendants' activities, products or services with any false or deceptive designation, representations, or descriptions of Defendants or of their activities, whether by symbols, words, designs, or statements, which would damage or injure Google or its customers or users, or would give Defendants an unfair competitive advantage or result in deception of consumers; and

39. Acting in any other manner that suggests in any way that Defendants' activities, products, or services come from or are somehow sponsored by or affiliated with Google, or passing off Defendants' activities, products, or services as Google's.

IT IS FURTHER ORDERED that, pursuant to the All Writs Act, Google may serve this Order on the persons or entities hosting or providing services related to the domains identified in Appendix A, requesting that those persons and entities take their best efforts to implement the following actions:

40. Take reasonable steps to identify incoming and/or outgoing Internet traffic on their respective networks that originates or is being sent from or to the domains identified in Appendix A;

41. Within three (3) business days of receipt of this Order, or as soon as practicable, take reasonable steps to block and/or disrupt access of incoming and/or outgoing Internet traffic or communications on their respective networks that originates and/or is being sent from or to the domains identified in Appendix A by Defendants or Defendants' representatives or resellers, except as explicitly provided for in this Order;

42. Take other reasonable steps to block and/or disrupt access of such traffic to and/or from any other IP addresses, domains, or Internet channels to which Defendants may move the Darcula infrastructure, including those identified by Google in an amendment to Appendix A, to ensure that Defendants cannot use such infrastructure to facilitate and expand the use of Magic Cat or continue to perpetrate illegal acts;

43. Make the computers, servers, electronic data storage devices, software, data, or media assigned to or otherwise associated with the domains set forth in Appendix A and make them inaccessible from any other computer on the Internet, any internal network, or in any other manner, to Defendants, Defendants' representatives, and all other persons, except as otherwise ordered herein;

44. Completely, and until further order of this Court, suspend all services to Defendants or Defendants' representatives or resellers associated with the domains set forth in Appendix A;

45. Should a provider identify any content and/or software hosted at the domains listed in Appendix A that it reasonably believes is not associated with Defendants, the provider shall preserve any such content and/or software; and contact Google's counsel, Laura Harris, at King & Spalding LLP, 1290 Avenue of the Americas, 14th Floor, New York, New York 10104-0101, and lharris@kslaw.com, within one (1) business day;

46. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives, and refrain from publicizing this Order until the steps required by this Order are executed in full, except as necessary to communicate with hosting companies, data centers, Google, or other ISPs to execute this Order;

47. Not enable, and take all reasonable steps to prevent, any circumvention of this Order by Defendants or Defendants' representatives associated with the domains listed in

Appendix A, including without limitation enabling, facilitating, and/or allowing Defendants or Defendants' representatives or resellers to rent, lease, purchase, or otherwise obtain other services associated with those domains and IP addresses;

48. Preserve, retain, and produce to Google all documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or controlling the domains set forth in Appendix A, including any and all individual or entity names, mailing addresses, e-mail addresses, facsimile numbers, telephone numbers, or similar contact information, including but not limited to such contact information reflected in billing, usage, access, and contact records and all records, documents, and logs associated with the use of or access to such domains and IP addresses;

49. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order; and

50. Completely preserve the computers, servers, electronic data storage devices, software, data, or media assigned to or otherwise associated with the domain names set forth in Appendix A, and preserve all evidence of any kind related to the content, data, software or accounts associated with such domains, IP addresses, and computer hardware.

51. In determining the method and mechanism to disable content and software associated with Defendants, the relevant persons and/or entities shall reasonably confer with Plaintiff's counsel of record in this action.

IT IS FURTHER ORDERED that Google may amend Appendix A if it identifies other domains used by Defendants in connection with the Darcula Enterprise, including any such domains that might not yet exist, without further order of this Court.

IT IS FURTHER ORDERED, that, good cause having been shown, Google may effectuate service using alternative service, including service of process, by electronic means—including by email using any information available from web-hosting companies provided in connection with domain names used in the Darcula Schemes or identified by Google in its investigation; website publication; and/or other means ordered herein—shall be deemed effective as to Defendants through the pendency of this action.

IT IS FURTHER ORDERED, that, good cause having been shown, this Court shall extend the TRO for an additional nine days, until January 9, 2026. Google's request is not the result of any lack of diligence on its part but instead based upon the elaborate nature of Defendants' unlawful conduct and the need to disrupt that conduct over the holidays. Defendants will not be prejudiced by the extension Google seeks. Defendants do not have any legitimate interest that will be impaired by a brief extension of the TRO; they are being enjoined from engaging in conduct that is already prohibited by law.

Security for Temporary Restraining Order

IT IS FURTHER ORDERED that Google shall post bond in the amount of $75,000 to be filed with the Clerk. The Clerk shall accept Google's submission of $75,000 in satisfaction of this Order's bond requirement.

Hearing On Order to Show Cause

IT IS FURTHER ORDERED pursuant to Federal Rule of Civil Procedure 65(b), and good cause having been shown that a brief extension of the TRO is warranted, that Defendants shall appear before this Court on January 9, 2026, at 10:00 am to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against Defendants, enjoining the conduct temporarily restrained by the preceding provisions of this

Order. Good cause has been shown for this Order to remain in effect through the Preliminary Injunction hearing, absent further order from the Court, given the need for additional time to effectuate the disruption ordered herein in light of the upcoming holidays.

So ordered.

_____
United States District Judge

Date: _____

Time: _____

Place: _____

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC, *Plaintiff,* v. DOE 1 a/k/a YUCHENG CHANG and DOES 2–25, *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

INTRODUCTION

This is an application for an emergency *ex parte* temporary restraining order ("TRO") to disrupt a global criminal enterprise that has stolen personal and financial information from over a million victims already and exploited the trust and goodwill associated with the Google brand. Using novel software designed to facilitate large-scale "phishing" attacks with artificial intelligence ("AI") technology,[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 such as the United States Postal Service, toll collection agencies, large financial institutions, and even Google and YouTube. The spoofed websites often feature Google logos to further enhance the illusion of legitimacy.

Defendants are members of a criminal enterprise operating under the alias "Darcula" (the "Enterprise" or the "Darcula Enterprise") that built, promoted, and deployed its phishing-as-a-service software known as "Magic Cat." Magic Cat is an end-to-end toolkit designed to facilitate every aspect of a phishing cyberattack. Enterprise members coordinate with each other to identify potential victims, "phish" using deceptive text messages and ads, build fraudulent websites, steal victims' personal and financial information, and monetize that information through various means, including transferring funds from victims' accounts to themselves and selling the stolen information to other criminals for further illicit use.

The Darcula Enterprise has already stolen personal and financial information from millions of victims globally, including in the Southern District of New York. Cybersecurity researchers estimate that 70–80% of all fraudulent text messages from Chinese phishing groups between late-2023 and mid-2024 originated from the Enterprise. Thanks to the work of cybersecurity experts

[1] A "phishing" attack is a form of cyberattack that dupes victims into clicking on malicious links, often with false messages about a lost package or unpaid toll.

and journalists who alerted the public to the Darcula scheme, the Enterprise has reduced the scope of its phishing operations. But the threat remains. Google's investigation demonstrates that new Magic Cat-linked phishing websites continue to be created daily. Between September and December 2025, Google received more than 5,000 reports from its users about fraudulent messages they received containing known Darcula phishing domains. And because the Enterprise's infrastructure remains intact and available, it could return to its former scope at any moment.

This Court should grant Google's motion and issue the proposed TRO and order to show cause for a preliminary injunction. Google needs these injunctions to carry out its disruption plan, which will disable domains the Enterprise has used to spoof legitimate websites in its phishing schemes. This Court and others have issued injunctions to disrupt similar cybercriminal enterprises.[2] This requested injunctive relief will disrupt the Enterprise's fraudulent schemes and impede further criminal activity by preventing the Enterprise's ability to reach 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). Defendants are members of an integrated criminal enterprise who carry out phishing attacks to defraud unsuspecting targets in the United States. To facilitate their criminal schemes, they spoof Google websites, use Google's products (e.g., Google Messages) to deliver their fraudulent messages to Google's customers, and use Google's trademarks and service marks (as further defined herein, Google's "Marks") on their spoofed websites to trick unsuspecting victims into thinking those fake websites are legitimate. The Enterprises' criminal activities

[2] *See, e.g.*, *Google LLC v. Does 1–25*, No. 1:25-cv-09421 (S.D.N.Y. Nov. 12, 2025), ECF No. 18; *Google LLC v. Does 1–25*, No. 1:25-cv-04503 (S.D.N.Y. July 1, 2025), ECF No. 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).

therefore violate the Racketeer Influenced and Corrupt Organizations Act ("RICO"), the Lanham Act, and the Computer Fraud and Abuse Act ("CFAA") and irreparably harm Google.

To prevent irreparable harm, relief must be *ex parte*. Advance notice could render futile the very relief Google seeks by allowing Defendants the opportunity to relocate their malicious infrastructure and conceal evidence of their misconduct. Google also respectfully submits that there is good cause for the Court to extend the TRO to early January to effectuate the disruption over the holidays, which requires coordination and action with at least 15 registrars. If this Court grants the emergency injunctive relief requested, Google will provide Defendants with notice after executing the disruption (and before a preliminary injunction hearing) through service as requested in this motion.

BACKGROUND

Defendants Doe 1 a/k/a Yucheng Chang and Does 2–25 are cybercriminals and co-conspirators who are members of the Enterprise and operate the well-known "Darcula" phishing ring using a set of software tools known as "Magic Cat." Complaint ("Compl.") ¶¶ 14–17; Declaration of [redacted] ("Google Decl.") ¶¶ 15–22; Declaration of [redacted] ("Naxo Decl.") ¶¶ 16–21. Defendants are believed to be in China. Compl. ¶¶ 14–15; Google Decl. ¶ 28; Naxo Decl. ¶ 21. Members of the Enterprise license the software and coordinate with each other using dedicated Telegram channels and other electronic communications. Compl. ¶¶ 47–61; Naxo Decl. ¶¶ 18, 20. Some of the Darcula Enterprise's well-known schemes include text phishing scams mimicking messages from the United States Postal Service ("USPS"), state toll collection agencies, and large financial services companies. The Enterprise has also developed a website template designed to facilitate scams impersonating the YouTube Premium enrollment page. Compl. ¶¶ 75–77; Naxo Decl. ¶¶ 58–67. Many of these scams feature Google's trademarks and service marks to convince victims that the websites are legitimate and to turn over their sensitive

financial data. Compl. ¶¶ 28, 30, 37–38; Google Decl. ¶¶ 29–37. Google has devoted and continues to devote substantial financial resources to investigating the Darcula schemes, to develop measures to identify and prevent these phishing attacks on its platforms, and to remediate the harms caused by the Enterprise. Compl. ¶¶ 93, 97, 105; Google Decl. ¶¶ 42–43. Since March 2024, the Enterprise has disseminated approximately 90,000 phishing websites. Compl. ¶ 91; Naxo Decl. ¶ 20. Google's investigation shows that the Enterprise continues to create new phishing websites daily, and approximately 400 of these domains remain active. Compl. ¶ 93; Naxo Decl. ¶ 21.

A. The Magic Cat Software

A "phishing" scheme is a cyberattack that dupes targets into revealing sensitive information (such as login or credit card information) through deceptive emails, text messages, or websites. Compl. ¶ 24; Naxo Decl. ¶ 8. These schemes have been enormously profitable, as has licensing the infrastructure necessary to execute them. Phishing-as-a-Service ("PhaaS") is a business model that sells software and support services to facilitate phishing, making it relatively easy for those without technical expertise to create a phishing campaign. Compl. ¶ 28; Naxo Decl. ¶ 9.

The Magic Cat software is an example of this model. The Enterprise created Magic Cat to make phishing quick, easy, and effective—it is a "phishing for dummies" kit, with a prepackaged suite of all the tools needed to run a phishing campaign, including a platform to collect, organize, and share stolen personal and financial information. The Enterprise has also upgraded the Magic Cat software to enable even more features. Magic Cat V2 included hundreds of premade templates of fake websites spoofing well-known organizations, including Google. Compl. ¶ 33; Naxo Decl. ¶¶ 55–56, 67. The Enterprise introduced Magic Cat V3 earlier this year, which added website customization and generative AI tools that greatly expands the scope of Magic Cat's potential

fraudulent schemes. Compl. ¶ 35; Naxo Decl. ¶ 20. While the Enterprise's phishers were previously limited to a few hundred spoof website templates, the AI functionality now allows Magic Cat users with little technical proficiency to create a spoofed version of any website in minutes. Compl. ¶ 36; Naxo Decl. ¶ 17. With V3, an Enterprise member can simply input the URL for any website into the Magic Cat platform, and the AI will use the website's content to generate a nearly indistinguishable spoofed version of the site that then can be quickly customized for a phishing scheme with Magic Cat's tools. Compl. ¶ 35; Naxo Decl. ¶ 17. On the back-end, the Magic Cat software has keystroke logging capability, which opens a window to a victim's phone or device when a victim accesses one of the fake phishing websites and records that victim's entry of personal and financial account information in real-time. Compl. ¶ 41.

B. The Darcula Enterprise

The precise identities of the individuals in the Darcula Enterprise are unknown. Compl. ¶¶ 16–17; Google Decl. ¶ 28. But Google, Naxo, and others investigating the Darcula Enterprise have identified at least five interconnected threat groups that manage and participate in the Enterprise. Compl. ¶¶ 47–73; Naxo Decl. ¶ 18. These threat groups develop and use the Magic Cat software to carry out the Enterprise's schemes and depend on each other's specialized contributions to execute the phishing schemes—some of the members may even play multiple roles in the schemes. Compl. ¶ 47; Naxo Decl. ¶ 18. The Developer Group develops and updates the Magic Cat software. Compl. ¶¶ 48–53; Naxo Decl. ¶¶ 6, 20. The Administrative Group connects all the members of the Enterprise together by managing the online communities where members distribute Magic Cat and coordinate support and execution of specific schemes. Compl. ¶¶ 54–61; Naxo Decl. ¶¶ 18, 20. The Data Broker Group supplies mass lists of potential victims' contact information organized by country and location. Compl. ¶¶ 62–64; Naxo Decl. ¶¶ 6, 18, 88–

89. The Spammer Group executes methods of sending out text messages to potential victims en masse (often operating numerous automated cell phone banks) to phish for the victims' personal and financial information. Compl. ¶¶ 65–67; Naxo Decl. ¶¶ 18, 100–04. And finally, the Theft Group monetizes the stolen information and credentials, such as by loading virtual copies of the stolen credit cards into Apple Wallets and Google Wallets, which it then uses to make payments directly to the Enterprise through its tap-to-pay terminals and sells to other criminals on the dark web for further illicit use. Compl. ¶¶ 68–70; Naxo Decl. ¶¶ 102–04. Acting together, the threat actor groups develop and execute the Enterprise's numerous criminal phishing schemes. Compl. ¶¶ 71–72; Naxo Decl. ¶¶ 18, 20, 107.

C. The Darcula Enterprise's Criminal Schemes

The Enterprise uses Magic Cat to carry out numerous criminal phishing schemes, such as those disseminating fraudulent messages about package deliveries and unpaid tolls to lure potential victims to spoofed websites. Compl. ¶¶ 78–89; Naxo Decl. ¶¶ 22–26.

Delivery Scheme. In this scam, the Darcula Enterprise sends a text message—purportedly from the USPS, for example—telling the targets that they have an undelivered package. Compl. ¶ 82; Naxo Decl. ¶ 26. To "complete delivery," the text tells targets that they must pay a small delivery fee by clicking on the website link provided, which directs them to a spoofed USPS website. *Id.* Once on the website, targets are prompted to enter their personal and financial information. Compl. ¶¶ 82–83; Naxo Decl. ¶ 26. As they enter their information, the Magic Cat software simultaneously tracks their keystrokes; the targets need not even submit the payment for the Enterprise to acquire their information. *Id.*

Toll Scheme. The Enterprise's Toll Scheme works much the same way; the text indicates that the target has a past due toll violation and directs the target to pay the purported toll. Compl.

¶¶ 87–88; Naxo Decl. ¶ 22. The text directs targets to spoofed websites of state toll collection agencies, such as Florida's SunPass website for toll payments, to enter their personal financial information. Compl. ¶¶ 85–86; Naxo Decl. ¶¶ 22, 44–51. The Darcula websites are nearly indistinguishable from the legitimate websites they mimic. Compl. ¶¶ 30, 35; Naxo Decl. ¶ 6.

YouTube Scheme. The YouTube Scheme also includes a text to the victim, but in this iteration, the text lures the target to visit a website mimicking the YouTube Premium enrollment webpage with promises of a free trial. Compl. ¶¶ 75–77; Naxo Decl. ¶¶ 65–66. Once on the fake site, targets are directed to enter their financial information to receive the free trial. Compl. ¶ 76; Naxo Decl. ¶ 66.

D. The Darcula Enterprise Harms Google and the Public

The Darcula Enterprise harms not only the victims of phishing attacks but also Google, other spoofed organizations, and numerous others. The Darcula Enterprise steals phishing victims' money and personal information. Compl. ¶¶ 90–91; Google Decl. ¶¶ 21–22. The Enterprise also harms Google and other businesses whose logos or websites have been spoofed by damaging customer trust and goodwill. Compl. ¶¶ 101–04; Google Decl. ¶¶ 39–42. Specifically, the Enterprise has created and deployed templates of the YouTube Premium enrollment page and spoofed websites featuring Google's branding or logos (e.g., YouTube, Google Play) on the sign-in screen. Compl. ¶¶ 75–77, 100–02; Google Decl. ¶¶ 32, 34–35. Victims may view the presence of Google logos as an indicator that the website is safe or legitimate. Compl. ¶ 103; Google Decl. ¶ 37. The Darcula Enterprise is thus using the Google branding—and the goodwill associated with it—to convince victims to turn over their sensitive information. *Id.* The Enterprise's crimes have also compelled Google to devote substantial financial resources to investigate the Enterprise's phishing schemes, to develop measures to identify and prevent these phishing attacks on its

platforms, and to remediate the harms caused by the Enterprise. Compl. ¶ 8; Google Decl. ¶¶ 42–43. Despite these efforts, Google has been unable to confirm Defendants' true identities due to their use of aliases and dummy accounts. Compl. ¶ 16; Google Decl. ¶ 28.

The Enterprise's widespread phishing attacks across multiple industries show that it is a sophisticated group with significant reach. Compl. ¶¶ 71–72, 74; Naxo Decl. ¶¶ 18–20. Because Darcula makes phishing so easy, it is capable of causing staggering harm. Compl. ¶ 28; Naxo Decl. ¶ 17. Over the course of just seven months, the Darcula Enterprise stole nearly 900,000 credit card numbers from individuals across more than 200 countries, including individuals in the United States. Compl. ¶ 91; Naxo Decl. ¶ 20. While the Enterprise has reduced its operations and profile following public exposure by journalists and cybersecurity researchers, it continues to create new Magic Cat phishing domains daily. Compl. ¶ 93; Naxo Decl. ¶ 21. Google has identified activity related to Darcula on its own platforms and has taken (and continues to take) action to combat that activity. Compl. ¶¶ 100, 108; Google Decl. ¶¶ 40–43. For example, between September and December 2025, Google received more than 5,000 reports from its users about fraudulent messages they received containing the Darcula Enterprise's phishing domains. Compl. ¶ 124; Google Decl. ¶ 40. And the looming threat of more widescale phishing by the Darcula Enterprise remains. So long as the Enterprise continues to operate and maintain its infrastructure, it continues to inflict and threaten more damage every day. Compl. ¶ 108; Google Decl. ¶ 44. Without further disruption, the Enterprise will continue to conduct its phishing schemes and to generate revenue that it can reinvest in other criminal activities. Compl. ¶ 5; Naxo Decl. ¶ 6.

ARGUMENT

I. This Court Should Grant Google's Proposed Temporary Restraining Order 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 Global Mkts., Inc. v. VCG Special Opportunities Master Fund Ltd.*, 598 F.3d 30, 34–35 (2d Cir. 2010).

Courts balance the factors to grant preliminary relief "like a sliding scale," such that "more of one excuses less of the other." *Strougo v. Barclays PLC*, 194 F. Supp. 3d 230, 233 (S.D.N.Y. 2016) (cleaned up). That said, "[i]rreparable harm is the single most important prerequisite for relief." *Weaver v. Schiavo*, 750 F. App'x 59, 60 (2d Cir. 2019) (cleaned up). Here, each injunction factor weighs in Google's favor. 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).

Courts have granted preliminary relief in cases where, as here, the defendants include unknown persons or entities operating a phishing scheme to harm the plaintiff and the public. *See, e.g.*, *Microsoft Corp.*, 2022 WL 18359421, at *4; *CME Grp. Inc.*, 2019 WL 13252902, at *2; *Facebook, Inc. v. Fisher*, 2009 WL 5095269, at *1 (N.D. Cal. Dec. 21, 2009) (granting TRO where defendants operated a phishing scheme to steal login credentials).

This case is a quintessential candidate for emergency relief. 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.

Absent disruption, the Enterprise will continue to profit from its unlawful activities at the expense of Google and an ever-increasing number of victims.

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

The Enterprise's illegal activities create consumer confusion in the marketplace, tarnish Google's trademarks, injure its goodwill, and damage its reputation by falsely associating Google with the Enterprise's phishing schemes. Compl. ¶¶ 99–104; Google Decl. ¶¶ 38–40. 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). Here, Google has invested significant resources to develop strong brand recognition associated with its name, logos, and products. Compl. ¶¶ 11–13; Google Decl. ¶¶ 7, 12. The harm to Google is further compounded by the substantial financial resources Google has devoted and continues to devote to combat the Darcula Enterprise's phishing schemes. Compl. ¶ 99; Google Decl. ¶¶ 42–43.

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 consists of elusive cybercriminals who likely will take steps to avoid complying with any judgment. *See, e.g.*, *Drobbin v. Nicolet Instrument Corp.*, 631 F. Supp. 860, 912 (S.D.N.Y. 1986) ("Where 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."). Moreover, Google is entitled to a presumption of irreparable harm on showing, as Google does here, a likelihood of success on its claims under the Lanham Act. *Two Hands IP LLC v. Two Hands Am., Inc.*, 563 F. Supp. 3d 290, 300 (S.D.N.Y. 2021); *see* 15 U.S.C. § 1116(a).

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). Google not only raises serious questions going to the merits, but it is 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 and digital forensics firm. Each declaration details substantial evidence of Defendants' misconduct and the irreparable harm they have caused to Google and the public. Given the strength of this evidence, the likelihood of success weighs heavily in favor of granting relief.

(i) Google Is Likely to Succeed on its Lanham Act Claims.

Google has established that 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 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, and often incontestable registrations. *See* Google Decl. ¶ 35 (detailing Google's registrations for the relevant Marks). Defendants appropriate 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, confusion is the point: Defendants exploit Google's trustworthy and well-known Marks on their spoofed websites to trick their targets into falling for their scams. 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).[3]

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

[3] *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).

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) have caused injury to the plaintiff. *Church & Dwight Co. v. SPD Swiss Precision Diagnostics, GmBH*, 843 F.3d 48, 65 (2d Cir. 2016). False advertising claims thus contain two key components. "First (and obviously), a plaintiff bringing a false advertising claim must show falsity," either by demonstrating 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). Second, a plaintiff "must also demonstrate that the false or misleading representation involved an inherent or material quality of the product." *Id.* (quoting *Schering Corp. v. Pfizer Inc.*, 189 F.3d 218, 229 n.3 (2d Cir. 1999)). "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 Cable, Inc. v. DirectTV, Inc.*, 497 F.3d 144, 153 (2d Cir. 2007)).

Here, Defendants deceive internet users by featuring Google's Marks on their spoofed websites, falsely marketing their scam as bearing Google's approval or involvement. Compl. ¶¶ 101–04; Google Decl. ¶¶ 34–35, 37. That fraudulent marketing scheme easily satisfies the elements of false advertising. The representations are literally false because the spoofed 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. ¶¶ 105–07; Google Decl. ¶¶ 29–36. And the representations are material because they are critical to the success of the phishing operation. The only reason Defendants' schemes are successful is because their websites

appear to be real—they bear the marks of trusted institutions and brands like Google and YouTube. *See* Compl. ¶¶ 102–03; Google Decl. ¶ 37. The messages using Google's Marks are placed in interstate commerce on the internet. *See* Compl. ¶ 100; Google Decl. ¶¶ 32, 40–41. And the messages have caused 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 the scams and protect its Marks. *See* Google Decl. ¶¶ 42–43. Defendants have thus violated the Lanham Act in multiple ways, many times over. For all these reasons, Google's Lanham Act claims are likely to succeed on the merits.

(ii) Google Is Likely to Succeed on Its RICO Claim.

Google is likely to prevail on its RICO claim. 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. *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 Darcula 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 Magic Cat software and social media infrastructure, 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 Darcula Enterprise. *See id*.; *see also* Compl. ¶¶ 47–71; Naxo Decl. ¶¶ 18–20. Members of the Enterprise all 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 new members of the Enterprise and facilitates constant communication; others supply lists of potential victims' contact information; others specialize in strategies for sending out SMS messages; and yet others steal more of a victim's information and money after the Enterprise acquires phished credentials. *See id*. The Enterprise works together to implement its schemes; none of the schemes can generate revenue without the Enterprise members' cooperation. *See* Compl. ¶¶ 71–72; Naxo Decl. ¶ 18.

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. ¶¶ 114–16; Naxo Decl. ¶ 107. 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). Using the Magic Cat software, Defendants can choose from hundreds of fake website templates or leverage AI technology (courtesy of the Developer Group) to set up fraudulent phishing websites that are designed to appear identical to legitimate websites. Compl. ¶¶ 48–53; Naxo Decl. ¶ 17. They can then turn to the Enterprise's Telegram channels and other communications forums (operated by the Administrative Group) to coordinate phishing activities across the Data Broker, Spammer, and Theft Groups. Compl. ¶¶ 54–61; Naxo Decl. ¶¶ 18, 20. Through the Magic Cat 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)). 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 has presented numerous examples of the Enterprise's criminal conduct that clearly form a "pattern" within the meaning of the statute. Compl. ¶¶ 74–89, 94–95; Naxo Decl. ¶¶ 22–26. Indeed,

the Enterprise has stolen credit card information from tens of thousands of individuals in the United States between October 2023 and June 2024 alone through its fraudulent text messages directing those victims to its spoofed phishing websites. Compl. ¶ 91; Naxo Decl. ¶ 20. And there can be no doubt that the aims of the Darcula Enterprise—to perpetrate phishing schemes—are inherently unlawful.

4. Predicate Acts. To show that a defendant engaged in racketeering activity, a plaintiff must establish that the defendant committed one or more of the predicate acts 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.

The Darcula Enterprise committed wire fraud by "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, each time its members sent text messages to trick individuals in the United States into unknowingly submitting sensitive personal or financial information through misrepresentation and deception 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)). In a seven-month period in 2023 and 2024, more than 500,000 individuals in the United States clicked on the links in Defendants' fraudulent text messages, and nearly 40,000 of these individuals went on to unwittingly provide their credit card information to the Enterprise in the fraudulent websites the text messages lured them to. Compl. ¶ 91; Naxo Decl. ¶ 20. And between September and December 2025, over 5,000 Google Messages users reported to Google fraudulent messages they received from the Darcula Enterprise to perpetrate phishing schemes to steal money

from these targets. Compl. ¶ 124; Google Decl. ¶ 40. Defendants have committed wire fraud many times over.

5. Injury to Google's Business and Property. 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); *see also id.* (construing "injure" in Section 1964(c) to have its "ordinary meaning," which encompasses "damage of or to ... reputation" (cleaned up)). The injury to Google's business is an inherent component—and is the direct result—of the Darcula Enterprise's schemes. Those scams dupe their victims into turning over their sensitive information by mimicking YouTube and other trusted brands, government agencies, and financial institutions, relying on Google Marks to prey on consumer trust. Google must respond to remediate the business impact of the Darcula Enterprise's schemes. It has been forced to spend time (over 150 hours) and money investigating the schemes and pursuing other mitigation efforts. Compl. ¶ 108; Google Decl. ¶ 43. Defendants' RICO violations have injured Google's business or property.

(iii) Google Is Also Likely to Succeed on Its RICO Conspiracy Claim.

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(d). The overlapping links among the Defendants—including the use of the Magic Cat software, the chats from the Telegram group, and the methods used to deploy sophisticated and widespread schemes—demonstrate that the Enterprise formed an agreement to undertake the acts described above as part of a common scheme and conspiracy. Compl. ¶¶ 34–46, 54–61, 71, 74–89, 130; Naxo Decl. ¶¶ 18–

20. 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(c).

(iv) Google Is Likely to Succeed on its CFAA Claims.

Congress enacted the CFAA to combat computer-related crimes. *See, e.g.*, *United States v. Valle*, 807 F.3d 508, 525 (2d Cir. 2015). The Darcula Enterprise's phishing schemes involve "precisely the type of activity that the CFAA is designed to prevent." *See, e.g.*, Preliminary Injunction Order, *Google LLC v. Does 1–25*, No. 1:25-cv-09421 (S.D.N.Y. Dec. 1, 2025), ECF No. 27 at ¶ 11 (finding CFAA liability for a similar phishing scheme). Courts routinely grant injunctive relief under the CFAA. *See, e.g.*, *id.* at *4. The Enterprise has violated and is continuing to violate the CFAA.

The evidence shows that the Defendants have "knowingly and with intent to defraud traffic[ked] in … password[s] or similar information," which can be used to gain unauthorized access to computer systems, by transferring and selling victims' stolen financial information and credentials through Telegram channels and other online forums. 18 U.S.C. § 1030(a)(6); *Tracfone Wireless, Inc. v. Simply Wireless, Inc.*, 229 F. Supp. 3d 1284, 1297 (S.D. Fla. 2017) (plaintiff stated claim under § 1030(a)(6) where trafficking occurred over the internet and a telecommunications network). To "traffic" a password means to "transfer" it. 18 U.S.C. § 1029(e)(5) ("[T]raffic means transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of" the password."). After procuring phished credentials (including account authorization codes) by impersonating other entities, the Enterprise transfers or sells those credentials to other members of the Enterprise and other cybercriminals. Compl. ¶¶ 77, 89, 91; Naxo Decl. ¶¶ 6, 19.

And Google has shown that Defendants' CFAA violations have caused losses exceeding $5,000 to multiple persons within the course of a year, including the costs Google incurred investigating and responding to Defendants' widespread phishing schemes, Google Decl. ¶ 43, giving rise to Google's civil right of action "to obtain compensatory damages and injunctive relief or other equitable relief," 18 U.S.C. § 1030(g); *id.* § 1030(c)(4)(A)(i)(I); *see also Saunders Ventures, Inc. v. Salem*, 797 F. App'x 568, 572–73 (2d Cir. 2019); *Univ. Sports Publ'ns Co. v. Playmakers Media Co.*, 725 F. Supp. 2d 378, 387–88 (S.D.N.Y. 2010). Google is therefore likely to succeed on the merits of its CFAA claim.

C. The Balance of Equities Decidedly Favors a Temporary Restraining Order.

The equities also favor a TRO. The Enterprise commits crimes, defrauds the public, and injures Google. There is no conceivable reason why the Enterprise should be permitted to continue its illegal activities. *See, e.g.*, *Suber v. VVP Servs.*, 2021 WL 1101235, at *7 (S.D.N.Y. Mar. 23, 2021) (balance of hardships supported court's grant of an *ex parte* injunctive relief where the 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 the 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.*[4]

[4] *See, e.g.*, *Google LLC*, No. 1:25-cv-09421, ECF No. 18 at ¶¶ 6–7; *Microsoft Corp. v. Does 1–2*, 2024 WL 1708328, at *11 (E.D. Va. Jan. 10, 2024) ("Defendants would not suffer any hardship

D. The Public Interest Favors a Temporary Restraining Order.

Finally, a TRO would serve the public interest. The Darcula Enterprise has defrauded over a million victims, while using their ill-gotten funds to support further criminal schemes. *See* Compl. ¶¶ 1, 67–70; Naxo Decl. ¶¶ 20, 102–04. With each day, Defendants create new phishing websites to deceive more victims. The public interest is served by enforcing statutes designed to protect the public—such as RICO, the Lanham Act, and the CFAA—and thwarting criminal activity with no legitimate justification whatsoever. *See, e.g.*, *CME Grp. Inc.*, 2019 WL 13252902, at *3 (public interest is served by enforcing Lanham Act against phishing operation); *Microsoft Corp.*, 2022 WL 18359421, at *5 (similar for CFAA).

II. The Temporary Restraining Order Must Be *Ex Parte*.

Rule 65 authorizes courts to enter a TRO *ex parte* when the moving party sets forth facts that show an immediate and irreparable injury and why notice should not be required. Fed. R. Civ. P. 65(b)(l). Under this rule, an order may be issued without prior oral or written notice if (1) "specific facts in an affidavit or a verified complaint clearly show that immediate and irreparable injury, loss, or damage will result to the movant" before the adverse party can be heard and (2) "the movant's attorney certifies in writing any efforts made to give notice and the reasons why it should not be required." *Id.* 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. As such, even where specific notice could have been given to the adverse party, *ex parte* orders are proper when notice "appears to serve only to render fruitless further prosecution of the action." *In re Vuitton et*

---

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).

Fils S.A., 606 F.2d 1, 5 (2d Cir. 1979) (per curiam); *see also Granny Goose Foods, Inc. v. Bhd. of Teamsters*, 415 U.S. 423, 439 (1974).

In any event, Google does not presently know Defendants' true identities because they routinely deploy aliases and false identities in connection with their cybercrime; consequently, it cannot provide them with written or oral notice. Courts routinely grant *ex parte* relief in these circumstances. *See*, *e.g.*, *Google LLC*, No. 1:25-cv-09421, No. ECF 18 (granting *ex parte* TRO against nearly identical phishing scheme); *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'"); *Sapient Corp. v. Does 1–50*, 2018 WL 8221301, at *2 (N.D. Cal. Mar. 27, 2018) (in action to enjoin phishing scheme, "SapientRazorfish's request for ex parte relief is not the result of any lack of diligence on SapientRazorfish's part, but instead based on the nature of Defendants' unlawful conduct"). *Ex parte* relief is also routinely granted where, as here, defendants are engaged in technically sophisticated cybercrimes such as those the Darcula Enterprise perpetrates and are "likely to delete or to relocate" their harmful internet infrastructure, "destr[oy] or conceal[] . . . other discoverable evidence" of misconduct, and "warn their 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 also 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. 1:21-cv-10260

(S.D.N.Y. Dec. 27, 2021), ECF No. 8 (*Ex Parte* Temporary Restraining Order and Order to Show Cause Re: Preliminary Injunction).

This case presents the same danger and requires immediate relief. The Enterprise's technological sophistication and ability to conceal operations pose a significant risk (if not certainty) that they will attempt to relocate and hide evidence of their phishing operations if Google is required to find and give the Enterprise advance notice of the precise relief it seeks. *See* Google Decl. ¶ 47. 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, 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).

There is also good cause for the Court to set a hearing for Defendants to show cause in early January, with the TRO remaining in effect until that hearing. Google will effectuate the disruption over the holidays and expects that the requisite coordination and action from at least 15 registrars may take longer than usual. A court may extend a TRO beyond 14 days if it finds that there is good cause to do so. Fed. R. Civ. P. 65 (b)(2). Good cause exists "if the circumstances that supported the initial grant of the temporary restraining order" have not changed. *FTC v. Automators LLC*, 2023 U.S. Dist. LEXIS 150791, at *3 (S.D. Cal. Aug. 25, 2023) (collecting cases). Just this year, this Court extended a TRO to afford additional time to complete technical disruption plans. *See, e.g.*, Order Extending Temporary Restraining Order, *Google LLC v. Does 1–25*, No. 1:25-cv-04503, ECF No. 17 (S.D.N.Y. July 1, 2025). It should grant a brief extension of the TRO here as well.

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

Google also requests permission to serve Defendants, who are believed to reside in China, by alternative means under Federal Rule of Civil Procedure 4(f)(3). Compl. ¶¶ 14–15; Google Decl. ¶ 28. Google requests authorization to serve Defendants through (1) website publication, and (2) email using any information Google receives through disruption efforts and from web-hosting companies provided in connection with domain names used in the Darcula phishing operation and/or any email addresses identified through Google's investigation.

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). "It is well-settled that service by email on foreign defendants meets this standard in an appropriate case." *Elsevier, Inc. v. Siew Yee Chew*, 287 F. Supp. 3d 374, 379 (S.D.N.Y. 2018). Here, service through website publication and electronic messages is likely to be the most accurate and viable means of notice and service for these foreign cybercriminal Defendants. Other courts have routinely authorized service by website publication and/or email or electronic messaging in similar circumstances. *See*, *e.g.*, *Google LLC*, No. 1:25-cv-09421, ECF No. 18 (granting alternative service by website publication and email for foreign defendants involved in nearly identical phishing scheme); *Sapient Corp.*, 2018 WL 8221301, at *1; *Microsoft Corp. v. Does 1–18*, 2014 WL 1338677, at *3 (E.D. Va. April 2, 2014). And "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). Google therefore respectfully requests that the Court authorize alternative service under Rule 4(f)(3) using the proposed methods.

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 cyber infrastructure used by the Enterprise, thereby disrupting its schemes, and to preserve all evidence about Defendants and their websites. Google Decl. ¶¶ 47–48. This relief would include the disruption of any domains that the Enterprise may use in the future to perpetrate the phishing operation 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 (Mar. 27, 2018).

The narrowly tailored relief Google requests satisfies these requirements. *First*, requiring 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 fraud. Just as the surveillance authorized in *New York Telephone* could not have been accomplished without the participation of the telephone company, the reasonable cooperation of the third-party registrars is required 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). And *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 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 LLC*, No. 1:25-cv-09421, No. ECF 18 at 11; *Google LLC v. Does 1–25*, No. 25-cv-04503 (S.D.N.Y. Sept. 18, 2025), ECF No. 18; *Starovikov*, 2021 WL 6754263, at *1; *Microsoft Corp. v. Nady and Does 1–4*, No. 24-cv-02013 (E.D. Va. Nov. 13, 2024), ECF No. 16 at 10 (ordering domain

registries to ensure that defendant cannot use domains to engage in phishing); *Microsoft Corp. v. John Does 1–2*, No. 24-cv-02719 (D.D.C. Sept. 25, 2024), ECF No. 12 at 9 (similar).[5] To protect the public from the serious threat posed by the Magic Cat software and Darcula Enterprise, it is well 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 Google identifies additional entities associated with or domains used in connection with the Magic Cat software.

CONCLUSION

Google respectfully requests that this Court grant its motion for a TRO, a brief extension of that TRO until early January, 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.

[5] *Microsoft Corp. v. John Does 1–2*, No. 21-cv-00822 (E.D. Va. July 16, 2021), ECF No. 18 at 7 (ordering registries to take steps to prevent defendants from "accessing, modifying, transferring or using in any manner the domains"); *Microsoft Corp. v. Does 1–2,* No. 17-cv-01224 (E.D. Va. Oct. 27, 2017), ECF No. 26 at 8 (ordering registries to prevent transfer or modification of the domains).

Dated: December 17, 2025

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

Christine M. Carletta
Paul Weeks (*pro hac vice* to be submitted)
KING & SPALDING LLP
1700 Pennsylvania Avenue, NW, Suite 900
Washington, DC 20006-4707
Tel: (202) 737-0500
Fax: (202) 626-3737
ccarletta@kslaw.com
pweeks@kslaw.com

Sumon Dantiki (*pro hac vice* to be submitted)
BAKER MACKENZIE LLP
815 Connecticut Avenue, N.W.
Washington, DC 20006
Tel: (202) 452-7000
Fax: (202) 452-7074
sumon.dantiki@bakermckenzie.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 8,730 words in accordance with Local Rule 7.1(c).

Exhibit 4

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC, *Plaintiff,* v. DOE 1 a/k/a YUCHENG CHANG and DOES 2–25, *Defendants.*	Civil Action No.:

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

I, [redacted], declare as follows:

1. I am an Investigator in Google's CyberCrime Investigation Group ("CCIG"). I submit this declaration in support of Google's Motion for an *Ex Parte* Temporary Restraining Order and Order to Show Cause. I have personal knowledge of the matters discussed in this declaration, and if called as a witness, I could and would testify competently to the matters discussed in this declaration.

2. As a CCIG Investigator, I evaluate cybersecurity threats that target, or are discovered by cybercriminals' use of, Google products and services, including Android, Chrome, Google Search, YouTube, Google Cloud, Google Ads, Google Ad Manager, and Google Pay. As part of a broader Google effort, my team works to investigate cybersecurity threats and identify and attribute attacks to protect Google users, products, services, platforms, and assets from serious cyber threats, including phishing attacks. [redacted]. While at Google, I have participated in and directed numerous phishing investigations and operations to disrupt internet infrastructure used by cybercriminals.

3. Google has investigated a group of cybercriminals operating under the alias "Darcula" who use an end-to-end software called "Magic Cat" to perpetrate widespread phishing scams (the "Darcula Enterprise" or "Enterprise").

4. CCIG, working with other relevant Google teams, has assessed the activities of this phishing software and the impact it has on Google and users of Google products. The conclusions in this declaration are based on Google's investigation. As part of that investigation, we have concluded that the Darcula Enterprise's use of Magic Cat has caused significant damage to Google, its customers, and victims of Darcula phishing attacks. Magic Cat is a powerful software that

utilizes artificial intelligence ("AI") spoofing capabilities and has facilitated, and continues to facilitate, the exponential growth of phishing attacks worldwide and in the United States. It will continue to cause serious harm if it continues unimpeded.

I. Google Products and Background

5. Google is recognized as a worldwide leader in technology that offers a wide variety of products and services to governments, businesses, and consumers. Many of Google's consumer-facing products and services are available at no or low-cost. Google's mission is to organize the world's information and make it universally accessible and useful. Google has many different revenue streams, including revenue generated from delivering relevant, cost-effective online advertising; cloud-based solutions that provide Google's enterprise customers with infrastructure and platform services as well as communication and collaboration tools; and sales of other products and services, such as fees received for subscription-based products, applications ("apps") and in-app purchases, and devices.

6. We maintain our position at the forefront of multiple sectors through a sustained commitment to offering products that are both dependable and advanced, including ensuring our Google products are secure by default. Google has pioneered technologies used by millions of people including the following products or services:

a. **Android**: Android is an operating system created by Google that is designed to run on mobile devices, such as smartphones or tablets. Google has both a proprietary version that is used for official Google devices and also released a free version as open-source software. In this Declaration, where I refer to "Android," I am referring to Google's proprietary version.

b. **Chrome**: Chrome is a web browser created and operated by Google that runs on various operating systems, including on personal computers, smartphones, and tablets.

c. **Google Ads**: Google Ads is an online advertising platform through which advertisers can publish advertisements on various platforms including, for example, Google Search and YouTube.

d. **Google Ad Manager**: Google Ad Manager is a comprehensive ad management platform that allows publishers to sell ad space.

e. **Gmail**: Gmail is an email service.

f. **Google Cloud**: Google Cloud consists of a set of physical assets, such as computers and hard disk drives, and virtual resources, such as virtual machines, that are contained in data centers around the globe.

g. **Google Pay**: Google Pay is a digital wallet and online payment system that allows users to make safe and secure payments, send money, and manage their finances using their smartphones, tablets, or computers. Google Pay has built-in authentication, transaction encryption, and fraud protection to keep customers' money and personal information safe.

h. **Google Play**: Google Play is the official app store for certified devices running on the Android operating system and its derivatives, allowing users to browse and download apps developed with the Android software development kit and published through Google. Google Play also serves as a digital content store that offers millions of apps, games, books, and other products to more than 2.5 billion monthly users across over 190 markets worldwide.

i. **Google Search**: Google Search is an internet-based search engine that allows users to search for publicly accessible documents and websites indexed by Google's servers.

j. **Rich Communication Services ("RCS"):** RCS chats let users send messages over mobile data and Wi-Fi, share files and high-resolution photos. Messages sent using RCS chats use the RCS protocol, an industry standard for carrier messaging, and Google's RCS infrastructure. RCS chats between Google Messages are end-to-end encrypted by default to keep users' conversations secure.

k. **YouTube**: YouTube is an online video sharing platform.

7. Each of these products and services, among others, contributes to the value of Google's brand—one of the most prominent and valuable brands in the world. The word "Google" itself has become a verb. Google has achieved this level of brand recognition over the course of nearly three decades by focusing on delivering safe and quality products. Google also expends significant resources to maintain the quality of its brand including by providing extensive resources and guidelines governing the use of Google trademarks to ensure those trademarks are used to promote and not diminish Google's reputation. These efforts ensure that Google remains one of the world's most trusted technology brands.

II. Google's Commitment to Cybersecurity

8. For the past two decades, Google has made security the cornerstone of its business. Our commitment to security begins with our product strategy. The company does not simply respond to security incidents or plug security holes. Instead, Google works to eliminate entire classes of threats for users and businesses whose work depends on our services. We strive to keep our users safe by making our products secure by default—by using progressive layers of both

digital and physical protection to block malware and cyberattacks, and by employing the best engineers in the world.

9. Google dedicates significant resources to privacy and security incident response to mitigate cyberattacks. We also invest substantial resources in safety, security, and content review efforts to combat misuse of Google's services, trademarks, and unauthorized access to user data by third parties.

10. Google has allocated, and continues to allocate, substantial resources to restricting phishing communications and protecting users on the web and mobile devices. These include, among other things, developing and constantly improving spam filters, flagging suspicious communications for the user, incorporating two-step verification protections, publicly reporting known phishing websites, scanning email attachments, and preventing suspicious account sign-ins.

11. Google also has dedicated resources to thwarting attacks that result from the operation of phishing attacks. For example, Google's Safe Browsing technology examines billions of URLs per day looking for unsafe websites. Every day, Google discovers thousands of new unsafe sites, many of which are legitimate websites that have been compromised. When Google detects unsafe sites, it displays warnings on Google Search and in web browsers. This free tool allows users to search to see whether a website is currently dangerous to visit. Similarly, Google Security Checkup is a free tool that provides personalized, step-by-step guidance and recommendations to enhance the security of users' Google Accounts. It helps users review and manage activities such as signed-in devices, recent security events, and apps with access to the user's account, as well as ensuring two-step verification and account recovery options are set up correctly.

12. Because the cyber threat landscape is constantly evolving, Google has also devoted significant resources to detecting potential cybersecurity threats, rapidly countering them, and informing the broader information security community about them. Google's efforts in this area are constantly evolving. Since 2021, Google has, among other efforts, committed $10 billion to cybersecurity initiatives; introduced Google Cloud Confidential Computing, which keeps data encrypted while it is being processed and keeps it secure throughout its entire life cycle; created the Google Open Source Security Team to improve the security of the open source software that the world relies on; and introduced Protected Computing, which transforms how, when, and where data is processed to technically ensure users' privacy and safety.

13. CCIG is central to all these efforts and focuses on protecting users from cybercrime on Google's platforms, with a particular focus on efforts to combat online fraud, phishing, and malware.

14. CCIG's work has been essential to disrupting numerous major cybersecurity threats, including significant botnet threats such as Glupteba,[1] Cryptbot,[2] BadBox, and BadBox 2.0,[3] and phishing threats like Lighthouse[4] and Darcula.

[1] Royal Hansen & Halimah DeLaine Prado, *New action to combat cyber crime*, Blog.Google (Dec. 7, 2021), https://tinyurl.com/bde3v5fy.
[2] Mike Trinh & Pierre-Marc Bureau, *Continuing our work to hold cybercriminal ecosystems accountable*, Blog.Google (Apr. 26, 2023), https://tinyurl.com/pktmdsrc.
[3] Google, *We're taking legal action against the BadBox 2.0 botnet.*, Blog.Google (July 17, 2025), https://tinyurl.com/yc7jw5fm.
[4] Halimah DeLaine Prado, *A dual strategy: legal action and new legislation to fight scammers*, Blog.Google (Nov. 12, 2025), https://tinyurl.com/ycxbub5n.

III. Phishing-as-a-Service and Magic Cat

15. With other Google investigators, I investigate cybercrime campaigns like phishing-as-a-service ("PhaaS") that are perpetrated by threat actors targeting Google and its customers. In this role, I have investigated the Darcula Enterprise and its PhaaS campaign.

16. Phishing is a type of cyberattack in which cybercriminals send emails, text messages, or electronic messages that impersonate organizations—including Google, its brands, and its logos—or individuals in order to trick the recipient of the attack into turning over sensitive information like passwords, credit card numbers, or banking information.

17. PhaaS turns this criminal activity into a business model—cybercriminals sell software and support services to better facilitate phishing schemes. The software, also sometimes referred to as a "phishing kit," provides the infrastructure necessary to create a fake website (or other platform), send bulk text messages and emails to victims, and collect and store stolen personal and/or financial information. A typical phishing kit may include ready-made text message templates, fake website templates, and training videos on how to use the phishing software, making it relatively easy for those without technical expertise to create a phishing campaign. The kits are essentially a guide to phishing, and they rely on a variety of respected brands—including Google—to lure targets into believing they are interacting with a legitimate entity and trick victims into sharing sensitive personal and financial information with untrustworthy sources.

18. The Darcula Enterprise's phishing software, referred to as "Magic Cat," is composed of two complementary components. The first part, called the "darcula-suite" software, is the front-end software that is installed on the phishing kit user's computer and allows the user to make and revise phishing websites. The second part is a server-based program, called Magic Cat. This part allows users to deploy phishing sites and collect stolen information from victims.

Typically, the entire software package is referred to as "Magic Cat," so I will refer to the software as Magic Cat other than when I am specifically referring to the darcula-suite front-end software.

19. Phishing kits, like Magic Cat, make cybercrime easier for less technically skilled perpetrators to commit because they can rely on a product that does all the technical work for them. Additionally, these kits make cybercrime cheaper because cybercriminals do not need to expend significant financial resources to develop and scale their infrastructure. The PhaaS model is lucrative because it enables widespread and fast-paced phishing activities.

20. The Darcula Enterprise's Magic Cat software allows its network of scammers to create and deploy fraudulent websites—which spoof the legitimate websites of YouTube and other well-known organizations and businesses—with ease. The Darcula Enterprise distributes links to these spoofed websites in phishing attacks initiated through iMessages, RCS messages, and SMS messages.

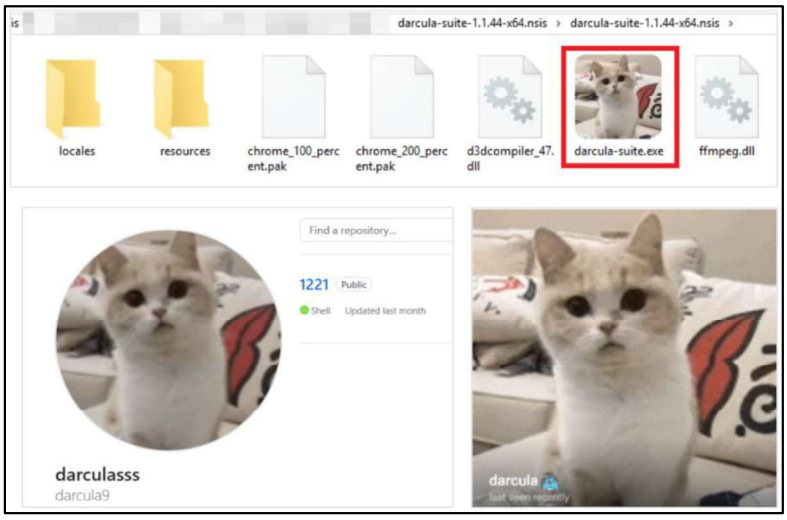
21. As victims type their personal and/or financial information into the spoofed website, Magic Cat collects the information and sends it directly to the Darcula Enterprise in real time.

22. Through the Darcula Enterprise's phishing operation, cybercriminals obtain the tools and know-how to attack Google customers and steal their personal and confidential financial information.

IV. Google's Investigation into the Darcula Enterprise's Phishing Scheme

23. Through its investigation of the Darcula Enterprise, Google obtained a copy of the source code for the Magic Cat software from VirusTotal on May 6, 2025. VirusTotal is a free, Google-owned online service that analyzes suspicious files, URLs, IP addresses, and domains for malware and threats using dozens of antivirus engines and threat intel feeds. Users can upload or

input items to be scanned, and the service aggregates results from multiple sources to provide a comprehensive safety assessment. The source code file "darcula-suite-1.1.44-x64.nsis.7z" (file size 93.81 MB) is available on VirusTotal with the first seen date of "2025-05-06 21:41:45 UTC." The source code file contains a desktop application called "darcula-suite" built with Electron framework (an open-source software framework that enables developers to build cross-platform desktop applications using web technologies like HTML, CSS, and JavaScript). The icon for the desktop application, shown below, is a cat picture that is identical to that used to identify other Darcula infrastructure, such as one of Darcula's Telegram administrative profile pictures and one of Darcula's GitHub repositories used to host the phishing templates.



24. VirusTotal logs the URLs outside of VirusTotal where the file is being used (known as an ITW URL or "In-the-Wild" URLs). Based on the ITW URLs for "darcula-suite," my team concluded that the source code file was hosted at "https://gitlab[.]com/magic-cat-v3/repo/-/raw/main/darcula-suite-1.1.44-x64.nsis.7z."

25. My team also acquired phishing templates from the Github repository located at the following URL: https[:]//github[.]com/feixiang8956/Darcula-phishing-CVV-Logs. We

downloaded the ".cat-page" file containing the phishing templates. The ".cat-page" file can be imported into the "darcula-suite" desktop application to create custom phishing pages.

26. Google has also worked to identify fraudulent website domains that were created using the Magic Cat software. By analyzing the source code and phishing templates, my team identified two unique fingerprints for Magic Cat. One of the files in the Magic Cat source code titled "/app/chunk/" contains two scripts ("DgZYu39z.js" and "IB9GIkLJ.js"). Together these scripts handle the encryption and decryption of messages sent and received from Magic Cat's command-and-control server via API endpoints and WebSockets. Both scripts have a unique name that never changes so they can be used to identify sites that use Magic Cat. In addition, both scripts contain references to "darcula."

27. My team provided the source code and phishing templates discussed above to our research partner NAXO for further investigation.

28. Based on cybersecurity researchers' public reporting about their investigations into the Darcula Enterprise, Google identified Gmail accounts used by members of the Darcula Enterprise. Based on billing instruments associated with these accounts, Google determined that an individual whose name is likely Yucheng Chang used some of these Gmail accounts. Google's analysis of the billing records associated with these Gmail accounts indicate that this individual resides in China. These findings from Google's investigation are consistent with the public reporting on the Darcula Enterprise, which identified an individual named "Yucheng C." as one of the leaders of the Enterprise.[5] In my experience, however, individuals involved in phishing schemes often use fake or stolen information; for that reason, Google does not know the Defendants' true identities.

[5] Martin Gundersen, *The Hunt for Darcula*, NRK (May 8, 2025), https://tinyurl.com/42bj5esj.

V. The Darcula Enterprise's Use of Google Trademarks and Products

29. The Darcula Enterprise uses free Google tools to carry out phishing schemes. For example, Darcula Enterprise members have created Gmail accounts to distribute the phishing messages to potential victims using Apple devices through iMessages linked to these Gmail accounts. And the Darcula Enterprise frequently distributes these phishing messages to potential victims using Android devices through Google Messages (through RCS).

30. The Darcula Enterprise also uses victims' stolen credit card information by adding those stolen credit cards to Google Wallets on burner Android devices.

31. The Darcula Enterprise's conduct violates Google's Terms of Service, which prohibit "accessing or using our services in fraudulent or deceptive ways, such as … phishing" or "creating fake accounts."[6] Although the identified accounts have been closed, I have directed my team to shut down any Enterprise-run Gmail accounts alongside Google's other disruption efforts.

32. Darcula also distributes hundreds of templates to create phishing websites that spoof the legitimate websites of YouTube as well as other reputable organizations and businesses, like the United States Postal Service, to encourage victims to enter their sensitive personal and financial information. Many of these spoofed phishing websites mimicking the websites of other reputable organizations and businesses also feature Google's trademarks for products such as YouTube or Google Play on the sign-in screen.

33. In addition, the most recent version of Magic Cat created and distributed earlier this year by the Darcula Enterprise uses AI to create a spoofed version of any website in minutes without any technical expertise required.

[6] Google, *Terms of Service* (last visited Dec. 14, 2025), https://tinyurl.com/4f59tyr9.

34. In April 2025, the Enterprise made a tutorial video demonstrating Magic Cat's new AI functionality. In that video, the Darcula Enterprise used Google's homepage (Google.com) to showcase how Magic Cat could create, in a matter of minutes, a spoofed version of the web page that could facilitate a new phishing scheme.

35. A list of Google trademarks the Darcula Enterprise has used without Google's permission in its cybercrime activities is attached as **Appendix B**.

36. The use of these logos violates Google's Rules for Proper Usage of its trademarks and brand features, which forbids, among other things, "display[ing] a Google Brand Feature on a site that violates any law or regulation," "display[ing] a Google Brand Feature in any manner that implies a relationship or affiliation with … Google," and "display[ing] a Google Brand Feature in a manner that is … misleading[] [or] infringing."[7] There are further requirements for the use of certain Google logos and icons. For example, Google's brand team must "review[] and fully approve[]" any use of the Google Play trademark.[8]

37. Due to Google's reputation of providing secure internet products, victims may view the presence of a Google trademark as an indicator that the website is safe or legitimate. The Darcula Enterprise is using the Google branding—and the goodwill associated with it—to convince victims to turn over their sensitive financial data.

VI. The Darcula Schemes Are Causing Harm to Google, Its Users, and the Public

38. The Darcula Enterprise's criminal actions have impacted Google, its users, and millions of other persons and entities.

[7] Google, *Rules for Proper Usage*, Brand Resource Ctr. (last visited Dec. 14, 2025), https://tinyurl.com/fppdbffw.
[8] Google, *Google Play Legal Requirements*, Partner Mktg. Hub (last visited Dec. 14, 2025), https://tinyurl.com/4vd29caf.

39. Phishing attacks created and deployed by the Darcula Enterprise harm victims by stealing their personal and financial information and their money. The Darcula Enterprise also harms Google by damaging customer trust and goodwill and forcing Google to invest significant time and resources into remediation efforts. Google has received thousands of complaints from customers related to phishing attacks, including those carried out by the Darcula Enterprise.

40. Between September 10 and December 3, 2025, over 5,000 Google Messages users—from the United States and other countries throughout the world—reported to Google fraudulent phishing messages they received from the Darcula Enterprise containing links to phishing website domains created through Magic Cat. For example:

a. On September 25, 2025, a U.S.-based Google Messages user reported receiving a phishing message from Defendants that stated, "We've detected multiple attempts to log into your account. If this was not you, please block it," followed by a link to a website domain created through Magic Cat to spoof the website of a U.S.-based financial institution.

b. On October 1, 2025, two different U.S.-based Google Messages users reported receiving a message from Defendants with identical text, each followed by a link to a different website domain created through Magic Cat to spoof the website of the same U.S.-based financial institution.

c. On October 5, 2025, another U.S.-based Google Messages user reported receiving a message from Defendants with identical text, again with a link to a website domain created through Magic Cat to spoof the website of the same U.S.-based financial institution.

d. On November 19, 2025, a U.S.-based Google Messages user reported receiving a phishing message from Defendants that stated, "Your updated 401(k) balance is ready to view. Please sign in for your most recent information," followed by a link to a website domain created through Magic Cat to spoof the website of a U.S.-based financial institution.

e. On November 27, 2025, another U.S.-based Google Messages user reported receiving a message from Defendants with identical text, again with a link to a website domain created through Magic Cat to spoof the website of the same U.S.-based financial institution.

41. More than 200 different known spoof website domains of the Darcula Enterprise were used across these more than 5,000 phishing messages to Google users. In response to the phishing messages, Google has taken action to block further Google Messages from being distributed by the phone numbers and/or accounts used to send these phishing messages.

42. Google has devoted (and continues to devote) substantial resources to detect, deter, and disrupt the Enterprise's activities. Google has done so because the use of Magic Cat poses a threat to Google's brand and reputation, and forces Google to devote resources to fraud-protection activities like flagging malicious websites and Google Messages sent through RCS.

43. Google has spent at least 150 hours investigating and remediating Defendants' activities, including engaging teams across four different countries. And Google will have to continue these efforts as the Darcula Enterprise's activities continue. The cost of investigating the Darcula Enterprise, assessing the damage it causes, and determining whether any remedial measures are needed, have far exceeded $5,000 in less than a one-year period from January 2025 to present.

44. Despite Google's best efforts, the Darcula Enterprise's continued cybercrime poses an imminent and irreparable injury to Google's business and reputation.

45. Beyond Google, the continued proliferation of phishing, smishing, and PhaaS is a threat to the public as whole.

46. Due to its sophisticated nature, I believe that if the Darcula Enterprise were given advance notice that the website domains and IP addresses they use in their phishing operation would be disabled, the Darcula Enterprise would take measures to ensure the phishing operation's survival and frustrate any disruption efforts.

47. Based on my experience and the information currently known, I believe the most effective way to address the harm caused by the Darcula Enterprise is to:

a. Direct the relevant domain registrars to suspend all known domain names and prevent them from being transferred, changed, or resold;

b. Direct the domain registrars to suspend all services to the Darcula Enterprise, not to warn or aid the Darcula Enterprise, and not to enable circumvention of the order; and

c. Block any efforts by the Defendants to create any additional domains.

48. I believe the only way to effectively disrupt the phishing operation and to address the harm caused to Google and the public is to take the steps described in the Proposed *Ex Parte* Temporary Restraining Order and Order to Show Cause. This relief will interrupt the Darcula Enterprise's harmful activities.

49. If the use of Magic Cat is not disrupted, it will continue to proliferate. The Darcula Enterprise will continue to generate revenue and will use those proceeds to expand its reach, producing more advanced software to facilitate and expand its criminal activity.

In accordance with 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct. Executed on December 16, 2025, in [redacted]

Appendix B

Appendix B
Google Registrations Implicated by the Darcula Enterprise

No.	Mark	Status / Dates
1	 RN: 4838524 SN: 86977379	Registered & Incontestable First Use: August 19, 2013 Filed: June 20, 2014 Registered: October 20, 2015
2	 RN: 5581035 SN: 86316342	Registered & Incontestable First Use: August 19, 2013 Filed: June 20, 2014 Registered: October 9, 2018
3	 RN: 5365541 SN: 86915697	Registered & Incontestable First Use: September 1, 2015 Filed: February 22, 2016 Registered: December 26, 2017
4	GOOGLE RN: 2806075 SN: 75978469	Renewed & Incontestable First Use: September, 1997 Filed: September 16, 1999 Registered: January 20, 2004 Last Renewal: January 20, 2024

No.	Mark	Status / Dates
5	GOOGLE RN: 6373292 SN: 87786172	Registered First Use: September, 1997 Filed: February 6, 2018 Registered: June 1, 2021
6	Google RN: 4058966 SN: 85222261	Renewed & Incontestable Registered: November 22, 2011 Last Renewal: November 22, 2021
7	Google RN: 5324610 SN: 86912587	Registered & Incontestable First Use: September 1, 2015 Filed: February 18, 2016 Registered: October 31, 2017
8	Google RN: 5324609 SN: 86912574	Registered & Incontestable First Use: September 1, 2015 Filed: February 18, 2016 Registered: October 31, 2017
9	GOOGLE PLAY RN: 5570801 SN: 85560994	Registered & Incontestable First Use: March 6, 2012 Filed: March 5, 2012 Registered: September 25, 2018
10	Google Play RN: 5628029 SN: 85563165	Registered & Incontestable First Use: April 14, 2016 Filed: March 7, 2012 Registered: December 11, 2018

Exhibit 5

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC, *Plaintiff,* v. DOE 1 a/k/a YUCHENG CHANG and DOES 2–25, *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 ("Google"). 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). 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 global criminal enterprise (the "Darcula 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 Google's TRO Motion, Memorandum of Law in Support of Its Motion for an *Ex Parte* Temporary Restraining Order and Order to Show Cause ("Memorandum of Law"), and supporting documents, the Darcula Enterprise has developed a software called "Magic Cat" that the Enterprise leverages to create and deploy large-scale phishing attacks. It includes templates for fake websites, domain set-up tools for those fake websites, and features designed to evade detection and lead victims to believe they are dealing with legitimate products.

Declaration of [redacted] in Support of Plaintiff's Motion for an *Ex Parte* Temporary Restraining Order and Order to Show Cause ("Naxo Declaration") ¶¶ 20–26, 42–67.

5. The Darcula Enterprise continues to create fraudulent websites daily that bear Google's trademarks and are causing irreparable harm to Google, its users, and the public. For example:

a. The Enterprise uses the Magic Cat software to create fake websites that resemble, for example, toll collection websites, that it uses to collect victims' financial and personal information. *Id.* ¶ 67. Those sites often use Google logos and trademarks to mimic legitimate sites. *Id.* ¶¶ 67, 80. Fooled by this resemblance, victims will then enter their personal financial information, like a credit card or bank account information.

b. The Darcula Enterprise collects and stores victims' information through the Magic Cat software. *Id.* ¶¶ 6, 17. The Enterprise members can then either exploit that information themselves, sell that information to other cybercriminals, or both. *Id.* ¶ 19.

6. Certain domains associated with web registrars have been identified as phishing websites created with the Magic Cat software. Those domains are set forth in **Appendix A** to the Naxo Declaration.

7. To disrupt the Darcula Enterprise and its phishing schemes, Google seeks to shut down domains created using the Magic Cat software. To suspend the infrastructure on which the Enterprise relies, Google must act quickly and coordinate with multiple domain registrars.

8. It is critical to implement this plan without notice to Defendants because, with notice, Defendants could destroy evidence of their activities and move their infrastructure to new domains to continue new versions of the schemes and frustrate efforts to disrupt them.

9. I have been informed that Google employees investigating Darcula, including Google's CyberCrime Investigation Group ("CCIG"), have attempted to identify the true identities of all responsible Defendants but have been unable to do so. Based on my experience on prior similar matters and on Google's research, Defendants may have provided contact information to web hosting companies during the domain-name registration process, which could potentially include mailing addresses, email addresses, facsimile numbers, and telephone numbers that could identify additional defendants.

10. In my experience, Defendants provide fake mailing addresses to registrars and web-hosting companies. Defendants are more likely to provide real email addresses so that they receive any notifications regarding service disruptions and to ensure they receive communications regarding registration expiration or other issues tied to the continued function of their domains.

11. Google has not attempted to provide notice of the TRO Motion to Defendants and should not be required to provide notice at this time.

12. As discussed more fully in Google's accompanying TRO Motion and Memorandum of Law, Google is likely to prevail on the merits of this case. Defendants are operating a worldwide criminal enterprise using the Magic Cat software; they are using technology that can be easily concealed and destroyed; and they have inflicted and are continuing to inflict harm on individuals 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 Darcula Enterprise by destroying business records, modifying the Magic Cat software, and otherwise 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

13. On behalf of Google, once the disruption plan reflected in the proposed TRO has been substantially completed, King & Spalding plans to attempt to provide notice of the pleadings, TRO Motion and supporting papers, and any TRO or preliminary injunction hearing to Defendants in the following ways: (A) by serving notice to email addresses associated with Defendants to the extent any email address information is available from web-hosting companies provided in connection with domain names used in the Darcula Enterprise's schemes or any email addresses identified through Google's investigation; and (B) by serving notice via website publication.

14. Defendants are believed to reside in China. Though China is a party to the Hague Convention on the Service Abroad of Judicial and Extra Judicial Documents, U.S. Dep't of State, *China Judicial Assistance Information*, https://tinyurl.com/dutau8dc (last visited Dec. 16, 2025), "[t]he Hague Convention is not the exclusive means for obtaining discovery from a foreign entity. Nor is the Convention necessarily the means of first resort," *First American Corp. v. Price Waterhouse LLP*, 154 F.3d 16, 21 (2d Cir. 1998) (internal citations omitted). And, in any event, Federal Rule of Civil Procedure 4(f) does not require service through the Hague Convention. *Elsevier, Inc. v. Siew Yee Chew*, 287 F. Supp. 3d 374, 377 (S.D.N.Y. 2018) ("[T]he rule does not require a party to serve process by the means specified in subsections 4(f)(l) and (f)(2) before a court permits alternative service by 'other means' under Rule 4(f)(3).").

A. Service to Email Addresses Associated with Defendants

15. King & Spalding will attempt to provide notice of any TRO and preliminary injunction hearing to Defendants on Google's behalf. King & Spalding will also attempt to serve

the Complaint to Defendants by sending the pleadings to email addresses associated with Defendants, provided by Defendants to the internet domain registrars, or relevant email addresses otherwise revealed by Google's investigation.

B. Service by Website Publication

16. King & Spalding will also attempt to provide notice of the pleadings, along with any TRO or preliminary injunction hearing, by publishing those materials on a publicly accessible website. King & Spalding will publish such notice on the website for a period of six months.

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 December 17, 2025, in New York, New York.

/s/ Laura Harris
Laura Harris

Exhibit 6

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC,

Plaintiff,

v.

DOE 1 a/k/a YUCHENG CHANG and DOES 2–25,

Defendants.

Civil Action No.: 25-cv-10440 (JSR)

[PROPOSED] *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

Plaintiff Google LLC ("Google" or "Plaintiff") has filed a Complaint for injunctive and other relief to stop Defendants Doe 1 a/k/a Yucheng Chang and Does 2–25, a criminal enterprise (the "Darcula Enterprise" or the "Enterprise"), from using novel software to facilitate large-scale phishing attacks that have harmed over one million victims, including Google.

Google filed a Complaint alleging claims under (1) the Racketeer Influenced and Corrupt Organizations Act ("RICO"), 18 U.S.C. § 1962(c)–(d) (Count I); (2) the Lanham Act, 15 U.S.C. §§ 1114(1), 1125(a)(1)(A), 1125(a)(1)(B) (Count II); and (3) the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a)(6) (Count III). Google has moved under seal and *ex parte* for a temporary restraining order and an order to show cause why a preliminary injunction should not issue under Federal Rule of Civil Procedure 65 and 28 U.S.C. § 1651.

THE COURT HEREBY FINDS THAT:

1. This Court has federal-question jurisdiction over Google's claims under RICO, the Lanham Act, and the CFAA pursuant to 28 U.S.C. § 1331.

2. This Court has personal jurisdiction over Defendants because:

a. Defendants have intentionally targeted and harmed Google, a company based in the United States. Defendants also have engaged in intentional, wrongful, illegal, and/or tortious acts, the effects of which Defendants intended to and knew would be felt in the United States and New York. Google does business in New York and has done business in New York for many years, including in this District.

b. Defendants have affirmatively directed actions at the United States, including this District, and Defendants attempted to phish and have successfully phished personal and financial information from victims within this District and New York State.

c. Defendants have used Google's trademarks as part of fake websites used to solicit victims' personal and financial information within this District and New York State, and have directed multiple forms of electronic communication to user devices in this District and New York State.

3. Venue is proper in this judicial district under 28 U.S.C. § 1391(c)(3) because Defendants are not residents of the United States and may be sued in any judicial district. Venue is also proper in this judicial district under 28 U.S.C. § 1391(b)(2) and 18 U.S.C. § 1965(a) because a substantial part of the events or omissions giving rise to Google's claims occurred in this judicial district, because a substantial part of the harm caused by Defendants has occurred in this judicial district, and because Defendants transact their affairs in this judicial district. Moreover, Defendants are subject to personal jurisdiction in this judicial district, and no other venue appears to be more appropriate.

4. The Complaint pleads facts with the specificity required by the Federal Rules of Civil Procedure and states claims against Defendants for violations of (1) RICO, 18 U.S.C.

§ 1962(c)–(d) (Count I); (2) the Lanham Act, 15 U.S.C. §§ 1114(1), 1125(a)(1)(A), 1125(a)(1)(B) (Count II); and (3) the CFAA, 18 U.S.C. § 1030(a)(6) (Count III).

Temporary Restraining Order Factors

5. The Court finds that Google has established each of the factors required for a temporary restraining order: (1) specific facts in declarations show that Google is likely to suffer immediate, irreparable harm before Defendants can be heard; (2) Google is likely to succeed on the merits and/or has established a substantial question as to the merits; (3) the balance of hardships tips in Google's favor; and (4) a temporary restraining order serves the public interest. *Citigroup Global Mkts., Inc. v. VCG Special Opportunities Master Fund Ltd.*, 598 F.3d 30, 34–35 (2d Cir. 2010); Fed. R. Civ. P. 65(b)(l)(A).

Irreparable Harm

6. Google has established by specific facts that in the absence of a temporary restraining order, it will suffer immediate, irreparable harm before Defendants can be heard in opposition. Defendants—through their operation of the Darcula Enterprise to participate in and carry out numerous criminal phishing scams (the "Darcula Schemes")—have threatened the security of the Internet and are causing ongoing and irreparable harm to Google and the public by using phishing attacks to steal personal and financial information, defrauding unsuspecting targets, impairing Google's reputation and goodwill, and causing Google (and numerous others) unrecoverable financial losses. Until the Darcula Schemes are disrupted, the Enterprise will continue to profit from its unlawful activities at the expense of Google and members of the public.

7. Defendants' conduct is injuring Google's goodwill and damaging its reputation by falsely associating Google with fraud perpetrated by the Darcula Enterprise, and injuries to goodwill and reputation constitute irreparable harm. Google has suffered and continues to suffer

economic losses from the Darcula Schemes because Google has expended (and continues to expend) substantial financial resources into developing strong brand recognition associated with its name, logos, and products, and investigating and combat Darcula Schemes and to identify measures necessary to remediate the harms caused by the Darcula Schemes. These injuries constitute irreparable harm, including because Google has shown a likelihood that Defendants would take steps to avoid complying with any judgment.

Likelihood of Success on the Merits

8. Google has demonstrated that its Complaint presents a substantial question as to each of its claims and that it is likely to succeed on the merits of its claims. *See Sterling v. Deutsche Bank Nat'l Tr. Co. as Trs. for Femit Tr. 2006-FF6*, 368 F. Supp. 3d 723, 727 (S.D.N.Y. 2019).

9. *The Lanham Act*. Google has shown a likelihood of success on the merits of its claims that Defendants violated and continue to violate the Lanham Act. Section 1114 of the Lanham Act prohibits infringement of a registered trademark or service mark. Infringement occurs when a valid, protectable mark is used in commerce and is likely to cause confusion, to cause mistake, or to deceive. 15 U.S.C. § 1114(1); *Virgin Enters. Ltd. v. Nawab*, 335 F.3d 141, 146 (2d Cir. 2003). Defendants violated this provision by exploiting Google's trustworthy, well-known, valid, protectable, and registered Marks on their spoofed websites to deceive consumers. Section 1125(a) prohibits false "designations of origin" that are likely to cause confusion as to the sponsorship 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, *Victorinox AG v. B & F System, Inc.*, 114 F. Supp. 3d 132, 139 (S.D.N.Y. 2015), so Google's section 1125(a)(1)(A) claim is 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) have caused injury to the plaintiff. *Church & Dwight Co. v. SPD Swiss Precision Diagnostics, GmBH*, 843 F.3d 48, 65 (2d Cir. 2016). Google has demonstrated that Defendants deceive Internet users by using Google's Marks on their spoofed websites. Google has shown that the representations are literally false because they are not from or endorsed by Google and that the representations are material because the Defendants' schemes are only successful because their websites appear to be real. The messages bearing Google Marks are placed in interstate commerce on the Internet, and Google has demonstrated injury to its goodwill and through costs to combat the Darcula Schemes. Google is thus likely to succeed on its Lanham Act claims.

10. *RICO*. Google has shown a likelihood of success on the merits of its claim that Defendants have violated and continue to violate the RICO statute, and that Defendants engaged in a RICO conspiracy.

a. Google has shown that Defendants are active participants in the operation and management of the Darcula Enterprise, which uses Magic Cat 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.

b. Google has established that Defendants constitute an enterprise. Defendants are associated-in-fact and share a common purpose defrauding victims into disclosing sensitive personal information, including financial account details, and stealing their money. Darcula Enterprise members all take part in directing the aspects of the scheme: some develop the Magic Cat software, architecture, and user interface; others manage an online community that recruits new Enterprise members; others supply potential victims' contact information; others specialize in phishing

strategies; and still others steal information and money from victims after the Enterprise phishes their credentials. Defendants collaborate to establish, grow, and manage the Darcula Enterprise, and coordinate to execute sophisticated phishing schemes.

c. Google has established that Defendants have engaged in a pattern of racketeering activity. *See* 18 U.S.C. § 1961(1), (5); *id.* § 2332b(g)(5)(B). The predicate acts include violations of the federal wire fraud statute, 18 U.S.C. § 1343. Defendants have, with intent to defraud and obtain money or property by means of false or fraudulent pretenses, committed wire fraud and continue to commit wire fraud by transmitting signals in interstate or foreign commerce for the purpose of deceiving device owners into submitting sensitive personal or financial information through deception, in violation of 18 U.S.C. § 1343.

d. Google has suffered injury to its business or property as a result of these predicate offenses by devoting substantial financial resources to investigate and remediate Defendants' criminal schemes in order to protect its goodwill and reputation.

e. Google has demonstrated that Defendants have engaged in a RICO conspiracy. The links among the Defendants—such as use of the Magic Cat software, communication over dedicated Telegram channels, and the methods used to deploy phishing schemes using Magic Cat and other Enterprise-controlled resources—demonstrate that the Enterprise formed an agreement as part of a common scheme and conspiracy.

11. *CFAA*. Google has shown a likelihood of success on the merits of its claim that Defendants violated and continue to violate the CFAA. Google has demonstrated that Defendants

have—knowingly and with intent to defraud—trafficked in passwords or similar information through which a computer may be accessed without authorization in interstate commerce through Telegram channels and other online forums in violation of 18 U.S.C. § 1030(a)(6). Defendants transfer and sell phished account credentials and authorization codes to other members of the Enterprise and other cybercriminals. Defendants' actions have caused loss to one or more persons in excess of $5,000 in a one-year period. *See id.* §§ 1030(g), 1030(c)(4)(A)(i)(I), including loss to Google, *see id.* § 1030(e)(11); *see also Saunders Ventures, Inc. v. Salem*, 797 F. App'x 568, 572–73 (2d Cir. 2019).

Balance of Hardships

12. The equities also favor a temporary restraining order. The Darcula Enterprise is defrauding consumers and injuring Google and continues to victimize more people each day. No countervailing factors weigh against a temporary restraining order. There is no legitimate reason why Defendants should be permitted to continue to weaponize Google's branding to defraud the public and commit cybercrimes.

Public Interest

13. Google has shown that the public interest favors granting a temporary restraining order.

14. The Darcula Enterprise has defrauded over one million victims, while using their ill-gotten funds to support other criminal schemes. With each passing day, Defendants deceive new victims. Protection from malicious cyberattacks and other cybercrimes is strongly in the public interest.

15. The public interest is also served by enforcing statutes designed to protect the public, including RICO, the Lanham Act, and the CFAA.

Good Cause for *Ex Parte* Relief

16. As discussed above, Google has set forth facts demonstrating immediate and irreparable harm. There is good cause to believe that if Defendants are provided advance notice of Google's TRO application or this Order, they would dissipate the Darcula Enterprise's infrastructure and resources, allowing them to continue their misconduct, and they would destroy, move, hide, conceal, or otherwise make inaccessible to the Court evidence of their misconduct.

Good Cause for Alternative Service

17. The Court finds good cause exists to grant alternative service of the filings in this matter by email using any information available from web-hosting companies provided in connection with domain names used in the Darcula Schemes and/or any email addresses identified through Google's investigation; website publication; and/or other means because Google establishes that traditional service methods would be futile. Given the online nature of Defendants' conduct, online alternative service is most likely to give Defendants notice of the filings pertaining to this lawsuit.

TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

IT IS HEREBY ORDERED that Defendants, their officers, agents, servants, employees, attorneys, and all others in active concert or participation with them, and each of the foregoing, who receive actual notice of this Order by personal service or otherwise ("Restrained Parties"), are temporarily restrained and enjoined, from, anywhere in the world:

18. Using, linking to, transferring, selling, exercising control over, or otherwise owning any interest in or accessing Magic Cat or the Internet domains through which the Darcula Enterprise perpetrates its phishing schemes, set forth in **Appendix A** to the Naxo Declaration in

Support of Plaintiff's Motion for an *Ex Parte* Temporary Restraining Order and Order to Show Cause ("Appendix A");

19. Attacking and compromising the security of the computers and networks of Google's customers;

20. Intentionally accessing protected computers and computer networks of Google's customers without authorization;

21. Sending messages or advertisements with links to malicious websites;

22. Engaging in phishing schemes;

23. Stealing or selling credentials from victims of phishing schemes;

24. Monitoring the activities of Google or Google's customers or stealing information from them;

25. Impersonating Google, its systems, products, and services;

26. Creating websites that falsely indicate that they are associated with Google, YouTube, or any other Google product or affiliate, through use of Google's trademarks and/or other false and/or misleading representations;

27. Misappropriating that which rightfully belongs to Google, Google's customers and users, or in which Google has a proprietary interest;

28. Configuring, deploying, operating, or otherwise participating in or facilitating the Darcula Enterprise described in the moving papers, including but not limited to the Internet domain names listed in Appendix A and through any other component or element of Defendants' illegal infrastructure in any location, including infrastructure Defendants may attempt to rebuild;

29. Delivering malicious code designed to steal credentials;

30. Selling access to the accounts of Google's customers;

31. Offering, promoting, or selling victims' credit cards or other financial information to others for use;

32. Using, transferring, exercising control over, or accessing any accounts used in the transfer of money or electronic currency, including cryptocurrency, or in the processing of card-based transactions, as a means to further Defendants' unlawful schemes; and/or

33. Undertaking any similar activity that inflicts harm on Google, Google's customers, or the public.

34. Upon service as provided for in this Order, Defendants and other Restrained Parties shall be deemed to have actual notice of the issuance and terms of the Order, and any act by any of the Restrained Parties in violation of any of the terms of the Order may be considered and prosecuted as contempt of court.

35. The Clerk of the Court is to issue a summons to Defendant Doe 1 a/k/a Yucheng Chang and a summons to Defendants Does 2–25 for Google to serve on Defendants.

36. Service of this Order shall be effectuated on or before January 4, 2025.

IT IS FURTHER ORDERED that the Restrained Parties are temporarily restrained and enjoined from:

37. Using and infringing Google's trademarks, including but not limited to Plaintiff's Google mark (RN: 5365541), Google Play mark (RN: 5628029), and YouTube mark (RN: 87984068), and/or other trademarks, trade names, service marks, or Internet domain addresses or names containing or infringing such trademarks, trade names or service marks, as set forth in **Appendix B** to the Google Declaration in Support of Plaintiff's Motion for an *Ex Parte* Temporary Restraining Order and Order to Show Cause, which contains Google's trademarks, trade names, service marks, or Internet domain addresses or names containing or infringing such trademarks,

trade names or service marks, or other intellectual property infringed as a result of Defendants' activities;

38. Using in connection with Defendants' activities, products or services with any false or deceptive designation, representations, or descriptions of Defendants or of their activities, whether by symbols, words, designs, or statements, which would damage or injure Google or its customers or users, or would give Defendants an unfair competitive advantage or result in deception of consumers; and

39. Acting in any other manner that suggests in any way that Defendants' activities, products, or services come from or are somehow sponsored by or affiliated with Google, or passing off Defendants' activities, products, or services as Google's.

IT IS FURTHER ORDERED that, pursuant to the All Writs Act, Google may serve this Order on the persons or entities hosting or providing services related to the domains identified in Appendix A, requesting that those persons and entities take their best efforts to implement the following actions:

40. Take reasonable steps to identify incoming and/or outgoing Internet traffic on their respective networks that originates or is being sent from or to the domains identified in Appendix A;

41. Within three (3) business days of receipt of this Order, or as soon as practicable, take reasonable steps to block and/or disrupt access of incoming and/or outgoing Internet traffic or communications on their respective networks that originates and/or is being sent from or to the domains identified in Appendix A by Defendants or Defendants' representatives or resellers, except as explicitly provided for in this Order;

42. Take other reasonable steps to block and/or disrupt access of such traffic to and/or from any other IP addresses, domains, or Internet channels to which Defendants may move the Darcula infrastructure, including those identified by Google in an amendment to Appendix A, to ensure that Defendants cannot use such infrastructure to facilitate and expand the use of Magic Cat or continue to perpetrate illegal acts;

43. Make the computers, servers, electronic data storage devices, software, data, or media assigned to or otherwise associated with the domains set forth in Appendix A and make them inaccessible from any other computer on the Internet, any internal network, or in any other manner, to Defendants, Defendants' representatives, and all other persons, except as otherwise ordered herein;

44. Completely, and until further order of this Court, suspend all services to Defendants or Defendants' representatives or resellers associated with the domains set forth in Appendix A;

45. Should a provider identify any content and/or software hosted at the domains listed in Appendix A that it reasonably believes is not associated with Defendants, the provider shall preserve any such content and/or software; and contact Google's counsel, Laura Harris, at King & Spalding LLP, 1290 Avenue of the Americas, 14th Floor, New York, New York 10104-0101, and lharris@kslaw.com, within one (1) business day;

46. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives, and refrain from publicizing this Order until the steps required by this Order are executed in full, except as necessary to communicate with hosting companies, data centers, Google, or other ISPs to execute this Order;

47. Not enable, and take all reasonable steps to prevent, any circumvention of this Order by Defendants or Defendants' representatives associated with the domains listed in

Appendix A, including without limitation enabling, facilitating, and/or allowing Defendants or Defendants' representatives or resellers to rent, lease, purchase, or otherwise obtain other services associated with those domains and IP addresses;

48. Preserve, retain, and produce to Google all documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or controlling the domains set forth in Appendix A, including any and all individual or entity names, mailing addresses, e-mail addresses, facsimile numbers, telephone numbers, or similar contact information, including but not limited to such contact information reflected in billing, usage, access, and contact records and all records, documents, and logs associated with the use of or access to such domains and IP addresses;

49. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order; and

50. Completely preserve the computers, servers, electronic data storage devices, software, data, or media assigned to or otherwise associated with the domain names set forth in Appendix A, and preserve all evidence of any kind related to the content, data, software or accounts associated with such domains, IP addresses, and computer hardware.

51. In determining the method and mechanism to disable content and software associated with Defendants, the relevant persons and/or entities shall reasonably confer with Plaintiff's counsel of record in this action.

IT IS FURTHER ORDERED that Google may amend Appendix A if it identifies other domains used by Defendants in connection with the Darcula Enterprise, including any such domains that might not yet exist, without further order of this Court.

IT IS FURTHER ORDERED, that, good cause having been shown, Google may effectuate service using alternative service, including service of process, by electronic means—including by email using any information available from web-hosting companies provided in connection with domain names used in the Darcula Schemes or identified by Google in its investigation; website publication; and/or other means ordered herein—shall be deemed effective as to Defendants through the pendency of this action.

IT IS FURTHER ORDERED, that, good cause having been shown, this Court shall extend the TRO for an additional nine days, until January 9, 2026. Google's request is not the result of any lack of diligence on its part but instead based upon the elaborate nature of Defendants' unlawful conduct and the need to disrupt that conduct over the holidays. Defendants will not be prejudiced by the extension Google seeks. Defendants do not have any legitimate interest that will be impaired by a brief extension of the TRO; they are being enjoined from engaging in conduct that is already prohibited by law.

Security for Temporary Restraining Order

IT IS FURTHER ORDERED that Google shall post bond in the amount of $75,000 to be filed with the Clerk. The Clerk shall accept Google's submission of $75,000 in satisfaction of this Order's bond requirement.

Hearing On Order to Show Cause

IT IS FURTHER ORDERED pursuant to Federal Rule of Civil Procedure 65(b), and good cause having been shown that a brief extension of the TRO is warranted, that Defendants shall appear before this Court on January 9, 2026, at 10:00 am to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against Defendants, enjoining the conduct temporarily restrained by the preceding provisions of this

Order. Good cause has been shown for this Order to remain in effect through the Preliminary Injunction hearing, absent further order from the Court, given the need for additional time to effectuate the disruption ordered herein in light of the upcoming holidays.

So ordered.

United States District Judge

Date: 12/17/25

Time: 6:40 p.m.

Place: New York, NY

Exhibit 7

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC,

Plaintiff,

v.

DOE 1 a/k/a YUCHENG CHANG and DOES 2–25,

Defendants.

Civil Action No.: 1:25-cv-10440-JSR

[PROPOSED] PRELIMINARY INJUNCTION ORDER

Plaintiff Google LLC has filed a Complaint for injunctive and other relief to stop Defendants Doe 1 a/k/a Yucheng Chang and Does 2–25, a criminal enterprise (the "Darcula Enterprise" or the "Enterprise"), from using novel software to facilitate large-scale phishing attacks that have harmed over one million victims, including Google.

Google filed a Complaint alleging claims under (1) the Racketeer Influenced and Corrupt Organizations Act ("RICO"), 18 U.S.C. § 1962(c)–(d) (Count I); (2) the Lanham Act, 15 U.S.C. §§ 1114(1), 1125(a)(1)(A), 1125(a)(1)(B) (Count II); and (3) the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a)(6) (Count III). Google moved *ex parte* for a temporary restraining order and an order to show cause why a preliminary injunction should not issue under Federal Rule of Civil Procedure 65 and 28 U.S.C. § 1651.

On December 17, 2025, this Court issued a Temporary Restraining Order ("TRO") and order for Defendants to show cause why a preliminary injunction should not issue.

THE COURT HEREBY FINDS THAT:

1. This Court has federal-question jurisdiction over Google's claims under RICO, the Lanham Act, and the CFAA pursuant to 28 U.S.C. § 1331.

2. This Court has personal jurisdiction over Defendants because:

a. Defendants have intentionally targeted and harmed Google, a company based in the United States. Defendants also have engaged in intentional, wrongful, illegal, and/or tortious acts, the effects of which Defendants intended to and knew would be felt in the United States and New York. Google does business in New York and has done business in New York for many years, including in this District.

b. Defendants have affirmatively directed actions at the United States, including this District, and Defendants attempted to phish and have successfully phished personal and financial information from victims within this District and New York State.

c. Defendants have used Google's trademarks as part of fake websites used to solicit victims' personal and financial information within this District and New York State, and have directed multiple forms of electronic communication to user devices in this District and New York State.

3. Venue is proper in this judicial district under 28 U.S.C. § 1391(c)(3) because Defendants are not residents of the United States and may be sued in any judicial district. Venue is also proper in this judicial district under 28 U.S.C. § 1391(b)(2) and 18 U.S.C. § 1965(a) because a substantial part of the events or omissions giving rise to Google's claims occurred in this judicial district, because a substantial part of the harm caused by Defendants has occurred in this judicial district, and because Defendants transact their affairs in this judicial district. Moreover, Defendants are subject to personal jurisdiction in this judicial district, and no other venue appears to be more appropriate.

4. The Complaint pleads facts with the specificity required by the Federal Rules of Civil Procedure and states claims against Defendants for violations of (1) RICO, 18 U.S.C.

§ 1962(c)–(d) (Count I); (2) the Lanham Act, 15 U.S.C. §§ 1114(1), 1125(a)(1)(A), 1125(a)(1)(B) (Count II); and (3) the CFAA, 18 U.S.C. § 1030(a)(6) (Count III).

Preliminary Injunction Order Factors

5. The Court finds that Google has established each of the factors required for a preliminary injunction: (1) irreparable harm; (2) a likelihood of success on the merits and/or has established a substantial question as to the merits; (3) the balance of hardships tips in Google's favor; and (4) a preliminary injunction serves the public interest. *Benihana, Inc. v. Benihana of Tokyo, LLC,* 784 F.3d 887, 895 (2d Cir. 2015); *see also Sterling v. Deutsche Bank Nat'l Tr. Co. as Trustees for Femit Tr. 2006-FF6*, 368 F. Supp. 3d 723, 727 (S.D.N.Y. 2019) ("The standard[s] for granting a temporary restraining order and a preliminary injunction pursuant to Rule 65 of the Federal Rules of [Civil] Procedure are identical.").

Irreparable Harm

6. Google has established that it will suffer immediate, irreparable harm if this Court denies its request for a preliminary injunction. Google has shown that Defendants—through their operation of the Darcula Enterprise to participate in and carry out numerous criminal phishing scams (the "Darcula Schemes")—have threatened the security of the Internet and are causing ongoing and irreparable harm to Google and the public by using phishing attacks to steal personal and financial information, defrauding unsuspecting targets, impairing Google's reputation and goodwill, and causing Google (and numerous others) unrecoverable financial losses. Until the Darcula Schemes are disrupted, the Enterprise will continue to profit from its unlawful activities at the expense of Google and members of the public.

7. Defendants' conduct is injuring Google's goodwill and damaging its reputation by falsely associating Google with fraud perpetrated by the Darcula Enterprise, and injuries to

goodwill and reputation constitute irreparable harm. Google has suffered and continues to suffer economic losses from the Darcula Schemes because Google has expended (and continues to expend) substantial financial resources into developing strong brand recognition associated with its name, logos, and products, and investigating and combat Darcula Schemes and to identify measures necessary to remediate the harms caused by the Darcula Schemes. These injuries constitute irreparable harm, including because Google has shown a likelihood that Defendants would take steps to avoid complying with any judgment.

Likelihood of Success on the Merits

8. Google has demonstrated that its Complaint presents a substantial question as to each of its claims and that it is likely to succeed on the merits of its claims. *See Sterling v. Deutsche Bank Nat'l Tr. Co. as Trs. for Femit Tr. 2006-FF6*, 368 F. Supp. 3d 723, 727 (S.D.N.Y. 2019).

9. *The Lanham Act.* Google has shown a likelihood of success on the merits of its claims that Defendants violated and continue to violate the Lanham Act. Section 1114 of the Lanham Act prohibits infringement of a registered trademark or service mark. Infringement occurs when a valid, protectable mark is used in commerce and is likely to cause confusion, to cause mistake, or to deceive. 15 U.S.C. § 1114(1); *Virgin Enters. Ltd. v. Nawab*, 335 F.3d 141, 146 (2d Cir. 2003). Defendants violated this provision by exploiting Google's trustworthy, well-known, valid, protectable, and registered Marks on their spoofed websites to deceive consumers. Section 1125(a) prohibits false "designations of origin" that are likely to cause confusion as to the sponsorship 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, *Victorinox AG v. B & F System, Inc.*, 114 F. Supp. 3d 132, 139 (S.D.N.Y. 2015), so Google's section 1125(a)(1)(A) claim is 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) have caused injury to the plaintiff. *Church & Dwight Co. v. SPD Swiss Precision Diagnostics, GmBH*, 843 F.3d 48, 65 (2d Cir. 2016). Google has demonstrated that Defendants deceive Internet users by using Google's Marks on their spoofed websites. Google has shown that the representations are literally false because they are not from or endorsed by Google and that the representations are material because the Defendants' schemes are only successful because their websites appear to be real. The messages bearing Google Marks are placed in interstate commerce on the Internet, and Google has demonstrated injury to its goodwill and through costs to combat the Darcula Schemes. Google is thus likely to succeed on its Lanham Act claims.

10. *RICO*. Google has shown a likelihood of success on the merits of its claim that Defendants have violated and continue to violate the RICO statute, and that Defendants engaged in a RICO conspiracy.

a. Google has shown that Defendants are active participants in the operation and management of the Darcula Enterprise, which uses Magic Cat 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.

b. Google has established that Defendants constitute an enterprise. Defendants are associated-in-fact and share a common purpose defrauding victims into disclosing sensitive personal information, including financial account details, and stealing their money. Darcula Enterprise members all take part in directing the aspects of the scheme: some develop the Magic Cat software, architecture, and user interface; others manage an online community that recruits new Enterprise members; others

supply potential victims' contact information; others specialize in phishing strategies; and still others steal information and money from victims after the Enterprise phishes their credentials. Defendants collaborate to establish, grow, and manage the Darcula Enterprise, and coordinate to execute sophisticated phishing schemes.

c. Google has established that Defendants have engaged in a pattern of racketeering activity. *See* 18 U.S.C. § 1961(1), (5); *id.* § 2332b(g)(5)(B). The predicate acts include violations of the federal wire fraud statute, 18 U.S.C. § 1343. Defendants have, with intent to defraud and obtain money or property by means of false or fraudulent pretenses, committed wire fraud and continue to commit wire fraud by transmitting signals in interstate or foreign commerce for the purpose of deceiving device owners into submitting sensitive personal or financial information through deception, in violation of 18 U.S.C. § 1343.

d. Google has suffered injury to its business or property as a result of these predicate offenses by devoting substantial financial resources to investigate and remediate Defendants' criminal schemes in order to protect its goodwill and reputation.

e. Google has demonstrated that Defendants have engaged in a RICO conspiracy. The links among the Defendants—such as use of the Magic Cat software, communication over dedicated Telegram channels, and the methods used to deploy phishing schemes using Magic Cat and other Enterprise-controlled resources—demonstrate that the Enterprise formed an agreement as part of a common scheme and conspiracy.

11. *CFAA*. Google has shown a likelihood of success on the merits of its claim that Defendants violated and continue to violate the CFAA. Google has demonstrated that Defendants have—knowingly and with intent to defraud—trafficked in passwords or similar information through which a computer may be accessed without authorization in interstate commerce through Telegram channels and other online forums in violation of 18 U.S.C. § 1030(a)(6). Defendants transfer and sell phished account credentials and authorization codes to other members of the Enterprise and other cybercriminals. Defendants' actions have caused loss to one or more persons in excess of $5,000 in a one-year period. *See id.* §§ 1030(g), 1030(c)(4)(A)(i)(I), including loss to Google, *see id.* § 1030(e)(11); *see also Saunders Ventures, Inc. v. Salem*, 797 F. App'x 568, 572–73 (2d Cir. 2019).

Balance of Hardships

12. The equities also favor a preliminary injunction. The Darcula Enterprise is defrauding consumers and injuring Google and continues to victimize more people each day. No countervailing factors weigh against a preliminary injunction. There is no legitimate reason why Defendants should be permitted to continue to weaponize Google's branding to defraud the public and commit cybercrimes.

Public Interest

13. Google has shown that the public interest favors granting a preliminary injunction.

14. The Darcula Enterprise has defrauded over one million victims, while using their ill-gotten funds to support other criminal schemes. With each passing day, Defendants deceive new victims. Protection from malicious cyberattacks and other cybercrimes is strongly in the public interest.

15. The public interest is also served by enforcing statutes designed to protect the public, including RICO, the Lanham Act, and the CFAA.

Good Cause for Alternative Service

16. The Court finds good cause exists to grant alternative service, including service of process, of the filings in this matter by email using any information available from web-hosting companies provided in connection with domain names used in the Darcula Schemes and/or any email addresses identified through Google's investigation; website publication; and/or other means because Google establishes that traditional service methods would be futile. Given the online nature of Defendants' conduct, online alternative service is most likely to give Defendants notice of the filings pertaining to this lawsuit.

PRELIMINARY INJUNCTION ORDER

IT IS HEREBY ORDERED that Defendants, their officers, agents, servants, employees, and attorneys, and all others in active concert or participation with them, and each of the foregoing who receive actual notice of this Order by personal service or otherwise ("Restrained Parties"), are preliminarily restrained and enjoined, from, anywhere in the world:

17. Using, linking to, transferring, selling, exercising control over, or otherwise owning any interest in or accessing Magic Cat or the Internet domains through which the Darcula Enterprise perpetrates its phishing schemes, set forth in **Appendix A** to the Naxo Declaration in Support of Plaintiff's Motion for an *Ex Parte* Temporary Restraining Order and Order to Show Cause ("Appendix A");

18. Attacking and compromising the security of the computers and networks of Google's customers;

19. Intentionally accessing protected computers and computer networks of Google's customers without authorization;

20. Sending messages or advertisements with links to malicious websites;

21. Engaging in phishing schemes;

22. Stealing or selling credentials from victims of phishing schemes;

23. Monitoring the activities of Google or Google's customers or stealing information from them;

24. Impersonating Google, its systems, products, and services;

25. Creating websites that falsely indicate that they are associated with Google, YouTube, or any other Google product or affiliate, through use of Google's trademarks and/or other false and/or misleading representations;

26. Misappropriating that which rightfully belongs to Google, Google's customers and users, or in which Google has a proprietary interest;

27. Configuring, deploying, operating, or otherwise participating in or facilitating the Darcula Enterprise described in the moving papers, including but not limited to the Internet domain names listed in Appendix A and through any other component or element of Defendants' illegal infrastructure in any location, including infrastructure Defendants may attempt to rebuild;

28. Delivering malicious code designed to steal credentials;

29. Selling access to the accounts of Google's customers;

30. Offering, promoting, or selling victims' credit cards or other financial information to others for use;

31. Using, transferring, exercising control over, or accessing any accounts used in the transfer of money or electronic currency, including cryptocurrency, or in the processing of card-based transactions, as a means to further Defendants' unlawful schemes; and/or

32. Undertaking any similar activity that inflicts harm on Google, Google's customers, or the public.

33. Upon service as provided for in this Order, Defendants and other Restrained Parties shall be deemed to have actual notice of the issuance and terms of the Order, and any act by any of the Restrained Parties in violation of any of the terms of the Order may be considered and prosecuted as contempt of court.

34. The Clerk of the Court is to issue a summons to Defendant Doe 1 a/k/a Yucheng Chang and a summons to Defendants Does 2–25 for Google to serve on Defendants.

IT IS FURTHER ORDERED that the Restrained Parties are preliminarily restrained and enjoined, from, anywhere in the world:

35. Using and infringing Google's trademarks, including but not limited to Plaintiff's Google mark (RN: 5365541), Google Play mark (RN: 5628029), and YouTube mark (RN: 87984068), and/or other trademarks, trade names, service marks, or Internet domain addresses or names containing or infringing such trademarks, trade names or service marks, as set forth in **Appendix B** to the Google Declaration in Support of Plaintiff's Motion for an *Ex Parte* Temporary Restraining Order and Order to Show Cause, which contains Google's trademarks, trade names, service marks, or Internet domain addresses or names containing or infringing such trademarks, trade names or service marks, or other intellectual property infringed as a result of Defendants' activities;

36. Using in connection with Defendants' activities, products or services with any false or deceptive designation, representations, or descriptions of Defendants or of their activities, whether by symbols, words, designs, or statements, which would damage or injure Google or its customers or users, or would give Defendants an unfair competitive advantage or result in deception of consumers; and

37. Acting in any other manner that suggests in any way that Defendants' activities, products, or services come from or are somehow sponsored by or affiliated with Google, or passing off Defendants' activities, products, or services as Google's.

IT IS FURTHER ORDERED that, pursuant to the All Writs Act, Google may serve this Order on the persons or entities hosting or providing services related to the domains identified in Appendix A, requesting that those persons and entities take their best efforts to implement the following actions:

38. Take reasonable steps to identify incoming and/or outgoing Internet traffic on their respective networks that originates or is being sent from or to the domains identified in Appendix A;

39. Within three (3) business days of receipt of this Order, or as soon as practicable, take reasonable steps to block and/or disrupt access of incoming and/or outgoing Internet traffic or communications on their respective networks that originates and/or is being sent from or to the domains identified in Appendix A by Defendants or Defendants' representatives or resellers, except as explicitly provided for in this Order;

40. Take other reasonable steps to block and/or disrupt access of such traffic to and/or from any other IP addresses, domains, or Internet channels to which Defendants may move the Darcula infrastructure, including those identified by Google in an amendment to Appendix A, to

ensure that Defendants cannot use such infrastructure to facilitate and expand the use of Magic Cat or continue to perpetrate illegal acts;

41. Make the computers, servers, electronic data storage devices, software, data, or media assigned to or otherwise associated with the domains set forth in Appendix A and make them inaccessible from any other computer on the Internet, any internal network, or in any other manner, to Defendants, Defendants' representatives, and all other persons, except as otherwise ordered herein;

42. Completely, and until further order of this Court, suspend all services to Defendants or Defendants' representatives or resellers associated with the domains set forth in Appendix A;

43. Should a provider identify any content and/or software hosted at the domains listed in Appendix A that it reasonably believes is not associated with Defendants, the provider shall preserve any such content and/or software; and contact Google's counsel, Laura Harris, at King & Spalding LLP, 1290 Avenue of the Americas, 14th Floor, New York, New York 10104-0101, and lharris@kslaw.com, within one (1) business day;

44. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives, and refrain from publicizing this Order until the steps required by this Order are executed in full, except as necessary to communicate with hosting companies, data centers, Google, or other ISPs to execute this Order;

45. Not enable, and take all reasonable steps to prevent, any circumvention of this Order by Defendants or Defendants' representatives associated with the domains listed in Appendix A, including without limitation enabling, facilitating, and/or allowing Defendants or Defendants' representatives or resellers to rent, lease, purchase, or otherwise obtain other services associated with those domains and IP addresses;

46. Preserve, retain, and produce to Google all documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or controlling the domains set forth in Appendix A, including any and all individual or entity names, mailing addresses, e-mail addresses, facsimile numbers, telephone numbers, or similar contact information, including but not limited to such contact information reflected in billing, usage, access, and contact records and all records, documents, and logs associated with the use of or access to such domains and IP addresses;

47. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order; and

48. Completely preserve the computers, servers, electronic data storage devices, software, data, or media assigned to or otherwise associated with the domain names set forth in Appendix A, and preserve all evidence of any kind related to the content, data, software or accounts associated with such domains, IP addresses, and computer hardware.

49. In determining the method and mechanism to disable content and software associated with Defendants, the relevant persons and/or entities shall reasonably confer with Plaintiff's counsel of record in this action.

IT IS FURTHER ORDERED that Google may amend Appendix A if it identifies other domains used by Defendants in connection with the Darcula Enterprise, including any such domains that might not yet exist, without further order of this Court.

IT IS FURTHER ORDERED that, because sufficient cause has been shown, alternative service, including service of process, by electronic means—including by email using any information available from web-hosting companies provided in connection with domain names used in the Darcula Schemes or identified by Google in its investigation; website publication;

and/or other means ordered herein—shall be deemed effective as to Defendants through the pendency of this action.

Security for Preliminary Injunction Order

IT IS FURTHER ORDERED that Google's submission of the $75,000 bond to the Clerk satisfied the requirements of this Court's TRO. No additional bond is necessary.

So ordered.

United States District Judge

Date: 2/9/26

Time: 9:10 a.m.

Exhibit 8

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----------X

Google LLC

Plaintiff(s),

- against -

Doe 1 a/k/a Yucheng Chang and Does 2–25

Defendant(s),

----------X

1:25 Civ. 10440 (JSR)

CLERK'S CERTIFICATE OF DEFAULT

I, TAMMI M. HELLWIG, Clerk of the United States District Court for the Southern District of New York, do hereby certify that this action was commenced on Dec. 17, 2025 **with the filing of a summons and complaint, a copy of the summons and complaint was served on defendant(s)** Doe 1 a/k/a Yucheng Chang and Does 2–25 **by personally serving** the Defendants in the manner ordered by the Court on Dec. 17, 2025, ***and proof of service was therefore filed on*** 1/8/2026, 2/19/26, ***Doc. #(s)*** 22, 35.

I further certify that the docket entries indicate that the defendant(s) has not filed an answer or otherwise moved with respect to the complaint herein. The default of the defendant(s) is/are hereby noted.

Dated: New York, New York

_____, 20___

TAMMI M. HELLWIG
Clerk of Court

By: _____
Deputy Clerk

Exhibit 9

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC, *Plaintiff,* v. DOE 1 a/k/a YUCHENG CHANG and DOES 2–25, *Defendants.*	Civil Action No.: 1:25-cv-10440-JSR

DECLARATION OF LAURA HARRIS IN SUPPORT OF
PLAINTIFF'S REQUEST FOR ENTRY OF DEFAULT

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 ("Google"). I am a member in good standing of the bar of New York. I make this declaration in support of Google's Request for Entry of Default Judgment against Defendants Doe 1 a/k/a Yucheng Chang and Does 2–25 ("Defendants") and of my own personal knowledge. If called as a witness, I could and would testify competently to the truth of the matters set forth herein.

2. A true and correct copy of Google's Request for Clerk's Certificate of Default is attached hereto as **Exhibit A**.

I. Defendants Are on Notice of This Action and Have Not Responded

3. In light of (a) Google's efforts to serve Defendants by email and publication on a publicly available website, magiccatdarculaserviceofprocess.com, beginning on January 4, 2026, (b) media coverage of this case that specifically mentions Google's claims against Defendants, and (c) Google's disruption of the phishing schemes, the Doe Defendants have been on notice of this action since at least January 4, 2026, and likely earlier. Yet, to date, none of the Defendants have appeared in connection with this lawsuit. Upon information and belief, the Defendants are not infants or incompetent persons. I base this conclusion in part on the fact that Defendants have engaged in sophisticated phishing schemes. I have seen no indication that Defendants are absent or have failed to file responsive pleadings due to present military service.

II. Service of Process

4. The Court found good cause to grant alternate service by email, mail, and publication on a publicly available website, pursuant to Rule 4(f)(3), and, as described more fully below, the Defendants have been properly served pursuant to the means authorized by the Court.

a. Identification of Defendants' Email Addresses

5. In connection with the disruption of the phishing scheme, Google served the Court's Temporary Restraining Order and Order to Show Cause ("TRO") on the third-party internet domain registrars (the "registrars") and internet registries (the "registries") for the domains listed in Appendix A. Many of the registrars provided contact information associated with the relevant accounts, including the email addresses used to register the domains in question.

6. Pursuant to the Court's orders, King & Spalding used this contact information to effectuate service on the Defendants. A true and correct copy of the Court's TRO issued December 17, 2025, is attached hereto as **Exhibit B**. A true and correct copy of the Court's Preliminary Injunction Order issued February 9, 2026, is attached hereto as **Exhibit C**. A true and correct copy of the Court's Memorandum Order issued February 9, 2026, is attached hereto as **Exhibit D**.

7. I oversaw Google's efforts to provide service and notice to the Defendants through the multiple channels identified below.

b. Service by Email

8. Google attempted to effectuate service by email, as authorized by the Court. Through its own investigation, Google identified 5 email addresses associated with domains listed in Appendix A and Google also received from the registrars 26 email addresses used to register domains listed in Appendix A. I oversaw the process of sending notice of this lawsuit to these email addresses.

9. Each email attempting to effectuate service was sent by an attorney at King & Spalding LLP with the following text:

> A lawsuit has been initiated against you in the United States District Court of the Southern District of New York. The following link contains copies of the restraining order, complaint, and related filings.

magiccatdarculaserviceofprocess.com

King & Spalding LLP

10. King & Spalding LLP received delivery failure notifications for four of the email addresses noting either that there was a problem with the recipients mailbox or that the address may not exist.

11. King & Spalding LLP attempted to effectuate service by email, as described above, on January 4, 2026, at approximately 7:26 p.m. ET.

12. On February 9, 2026, King & Spalding attempted to effectuate service of additional filings, including the Preliminary Injunction Order issued by the Judge that same day, to the email addresses previously mentioned. King & Spalding received delivery-failure notifications for 10 of the 31 email addresses noting that either the email address may not exist or was inactive.

13. On February 19, 2026, King & Spalding attempted to effectuate service of additional filings, including the Summons issued by the Clerk of Court that same day, to the email addresses previously mentioned. King & Spalding again received delivery failure notifications for 10 of the 31 email addresses.

c. Service by Publication

14. Google also attempted to effectuate service by publication through a publicly available website, as authorized by the Court.

15. On January 4, 2026, Google published the website magiccatdarculaserviceofprocess.com, which contains links to all relevant pleadings and orders as well as contact information for Google's counsel. That website is routinely updated.

16. The website prominently displays the following text:

> Plaintiff Google LLC ("Google") has sued Defendants Does 1-25 associated with the Internet domains listed in the pleading set forth below. Google alleges that

> Defendants have deployed a phishing-as-as-service model to facilitate and execute phishing attacks designed to steal personal and financial information, and Defendants have misused Google trademarks in their scheme. Google alleges that, through these actions, the Defendants have violated federal law. Google sought and received a temporary restraining order enjoining the Defendants from these and other activities and directing the third parties associated with Defendants' Internet domains to take all steps necessary to disable access to and operation of Magic Cat/Darcula-associated domains. Google intends to seek a preliminary injunction and other equitable relief. Full copies of the complaint, related filings, and orders from the Court are available below.
>
> NOTICE TO DEFENDANT: READ THESE PAPERS CAREFULLY! A hearing to show cause why the Court should not enter a Preliminary Injunction will be held on January 9, 2026 at 10 a.m.
>
> You must "appear" in this case or the other side will win automatically. To "appear" you must file with the court a legal document called a "motion" or "answer." The "motion" or "answer" must be given to the court clerk or administrator within 21 days of the date of first publication specified herein. It must be in proper form and have proof of service on Google's attorney, Laura Harris, King & Spalding LLP, 1290 Avenue of the Americas, 14th Fl., New York, NY 10104-0101. If you have questions, you should consult with your own attorney immediately.

17. A link to this website was also included in each service of process email. Attached hereto as **Exhibit E** is a true and correct copy of a printed copy dated March 2, 2026, of the publicly available website, magiccatdarculaserviceofprocess.com.

18. Attached as **Exhibit F** are true and correct copies of Google's certificates of service showing that the foregoing documents have been personally served on Defendants.

III. Additional Means of Notification

19. Upon information and belief, the Defendants also have actual notice of this proceeding given the impact of the TRO, the Preliminary Injunction Order, and Google's disruption efforts thereunder.

20. Following the Court's issuance of the TRO on December 17, 2025, Google began its efforts to disrupt the Internet domains associated with the Darcula Enterprise. As detailed in the

Court's Preliminary Injunction Order, *see* Ex. C, Google's efforts have led to the suspension or disruption of 325 of 392 currently known domains associated with the Darcula Enterprise.

21. Many news websites have published stories concerning this litigation. Below are just a few examples of this media coverage detailing the claims against the Defendants:

- Kevin Collier, *Google sues alleged Chinese scam group behind massive U.S. text message phishing ring*, NBC News (Dec. 17, 2025), https://www.nbcnews.com/tech/security/google-sues-chinese-scam-ring-e-zpass-usps-phishing-texts-rcna249469.

- Jeff Stone, *Google Sues Chinese 'Darcula' Group Over Alleged Phishing Scheme*, Bloomberg (Dec. 17, 2025), https://www.bloomberg.com/news/articles/2025-12-17/google-sues-chinese-darcula-group-over-alleged-phishing-scheme.

- Steve Weisman, *Google Sues Darcula: How The Tech Giant Is Using The Courts To Fight Cybercrime*, Forbes (updated Dec. 27, 2015), https://www.forbes.com/sites/steveweisman/2025/12/26/googles-sues-darcula-how-the-tech-giant-is-using-the-courts-to-fight-cybercrime/.

- Gintaras Radauskas, *Google sues another Chinese scam group over large phishing scheme*, Cybernews (Dec. 18, 2025), https://cybernews.com/security/google-cybercrime-chinese-gang-darcula/.

- Mudit Dube, *Google Sues Chinese Group Behind Massive Phishing Scam*, NewsBytes (Dec. 18, 2025), https://www.newsbytesapp.com/news/science/google-sues-chinese-group-behind-us-text-message-phishing-ring/story.

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

Executed on March 13, 2026, in New York, New York.

/s/ Laura Harris
Laura Harris

Exhibit A

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

Google LLC

Plaintiff(s)

vs.

Doe 1 a/k/a Yucheng Chang and Does 2–25,

Defendant(s)

Request for Clerk's Certificate of Default

Civil Case No.1:25-cv-10440-JSR

Pursuant to Fed. R. Civ. P. 55(a) and L.R. 55.1, Google LLC requests a Clerk's certificate of entry of default. Within in an accompanying affidavit, I affirm that the party against whom the judgment is sought:

1) is not an infant or incompetent person;

2) is not in the military service;

3) was properly served under Fed. R. C. P. 4 and proof of service having been filed with the court;

4) has defaulted in appearance in the above captioned action.

/s/ *Laura Harris*

Counsel for Plaintiff(s) / Plaintiff(s) Pro se

Exhibit B

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC,

Plaintiff,

v.

DOE 1 a/k/a YUCHENG CHANG and DOES 2–25,

Defendants.

Civil Action No.: 25-cv-10440 (JSR)

[PROPOSED] *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

Plaintiff Google LLC ("Google" or "Plaintiff") has filed a Complaint for injunctive and other relief to stop Defendants Doe 1 a/k/a Yucheng Chang and Does 2–25, a criminal enterprise (the "Darcula Enterprise" or the "Enterprise"), from using novel software to facilitate large-scale phishing attacks that have harmed over one million victims, including Google.

Google filed a Complaint alleging claims under (1) the Racketeer Influenced and Corrupt Organizations Act ("RICO"), 18 U.S.C. § 1962(c)–(d) (Count I); (2) the Lanham Act, 15 U.S.C. §§ 1114(1), 1125(a)(1)(A), 1125(a)(1)(B) (Count II); and (3) the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a)(6) (Count III). Google has moved under seal and *ex parte* for a temporary restraining order and an order to show cause why a preliminary injunction should not issue under Federal Rule of Civil Procedure 65 and 28 U.S.C. § 1651.

THE COURT HEREBY FINDS THAT:

1. This Court has federal-question jurisdiction over Google's claims under RICO, the Lanham Act, and the CFAA pursuant to 28 U.S.C. § 1331.

2. This Court has personal jurisdiction over Defendants because:

a. Defendants have intentionally targeted and harmed Google, a company based in the United States. Defendants also have engaged in intentional, wrongful, illegal, and/or tortious acts, the effects of which Defendants intended to and knew would be felt in the United States and New York. Google does business in New York and has done business in New York for many years, including in this District.

b. Defendants have affirmatively directed actions at the United States, including this District, and Defendants attempted to phish and have successfully phished personal and financial information from victims within this District and New York State.

c. Defendants have used Google's trademarks as part of fake websites used to solicit victims' personal and financial information within this District and New York State, and have directed multiple forms of electronic communication to user devices in this District and New York State.

3. Venue is proper in this judicial district under 28 U.S.C. § 1391(c)(3) because Defendants are not residents of the United States and may be sued in any judicial district. Venue is also proper in this judicial district under 28 U.S.C. § 1391(b)(2) and 18 U.S.C. § 1965(a) because a substantial part of the events or omissions giving rise to Google's claims occurred in this judicial district, because a substantial part of the harm caused by Defendants has occurred in this judicial district, and because Defendants transact their affairs in this judicial district. Moreover, Defendants are subject to personal jurisdiction in this judicial district, and no other venue appears to be more appropriate.

4. The Complaint pleads facts with the specificity required by the Federal Rules of Civil Procedure and states claims against Defendants for violations of (1) RICO, 18 U.S.C.

§ 1962(c)–(d) (Count I); (2) the Lanham Act, 15 U.S.C. §§ 1114(1), 1125(a)(1)(A), 1125(a)(1)(B) (Count II); and (3) the CFAA, 18 U.S.C. § 1030(a)(6) (Count III).

Temporary Restraining Order Factors

5. The Court finds that Google has established each of the factors required for a temporary restraining order: (1) specific facts in declarations show that Google is likely to suffer immediate, irreparable harm before Defendants can be heard; (2) Google is likely to succeed on the merits and/or has established a substantial question as to the merits; (3) the balance of hardships tips in Google's favor; and (4) a temporary restraining order serves the public interest. *Citigroup Global Mkts., Inc. v. VCG Special Opportunities Master Fund Ltd.*, 598 F.3d 30, 34–35 (2d Cir. 2010); Fed. R. Civ. P. 65(b)(l)(A).

Irreparable Harm

6. Google has established by specific facts that in the absence of a temporary restraining order, it will suffer immediate, irreparable harm before Defendants can be heard in opposition. Defendants—through their operation of the Darcula Enterprise to participate in and carry out numerous criminal phishing scams (the "Darcula Schemes")—have threatened the security of the Internet and are causing ongoing and irreparable harm to Google and the public by using phishing attacks to steal personal and financial information, defrauding unsuspecting targets, impairing Google's reputation and goodwill, and causing Google (and numerous others) unrecoverable financial losses. Until the Darcula Schemes are disrupted, the Enterprise will continue to profit from its unlawful activities at the expense of Google and members of the public.

7. Defendants' conduct is injuring Google's goodwill and damaging its reputation by falsely associating Google with fraud perpetrated by the Darcula Enterprise, and injuries to goodwill and reputation constitute irreparable harm. Google has suffered and continues to suffer

economic losses from the Darcula Schemes because Google has expended (and continues to expend) substantial financial resources into developing strong brand recognition associated with its name, logos, and products, and investigating and combat Darcula Schemes and to identify measures necessary to remediate the harms caused by the Darcula Schemes. These injuries constitute irreparable harm, including because Google has shown a likelihood that Defendants would take steps to avoid complying with any judgment.

Likelihood of Success on the Merits

8. Google has demonstrated that its Complaint presents a substantial question as to each of its claims and that it is likely to succeed on the merits of its claims. *See Sterling v. Deutsche Bank Nat'l Tr. Co. as Trs. for Femit Tr. 2006-FF6*, 368 F. Supp. 3d 723, 727 (S.D.N.Y. 2019).

9. *The Lanham Act.* Google has shown a likelihood of success on the merits of its claims that Defendants violated and continue to violate the Lanham Act. Section 1114 of the Lanham Act prohibits infringement of a registered trademark or service mark. Infringement occurs when a valid, protectable mark is used in commerce and is likely to cause confusion, to cause mistake, or to deceive. 15 U.S.C. § 1114(1); *Virgin Enters. Ltd. v. Nawab*, 335 F.3d 141, 146 (2d Cir. 2003). Defendants violated this provision by exploiting Google's trustworthy, well-known, valid, protectable, and registered Marks on their spoofed websites to deceive consumers. Section 1125(a) prohibits false "designations of origin" that are likely to cause confusion as to the sponsorship 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, *Victorinox AG v. B & F System, Inc.*, 114 F. Supp. 3d 132, 139 (S.D.N.Y. 2015), so Google's section 1125(a)(1)(A) claim is 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) have caused injury to the plaintiff. *Church & Dwight Co. v. SPD Swiss Precision Diagnostics, GmBH*, 843 F.3d 48, 65 (2d Cir. 2016). Google has demonstrated that Defendants deceive Internet users by using Google's Marks on their spoofed websites. Google has shown that the representations are literally false because they are not from or endorsed by Google and that the representations are material because the Defendants' schemes are only successful because their websites appear to be real. The messages bearing Google Marks are placed in interstate commerce on the Internet, and Google has demonstrated injury to its goodwill and through costs to combat the Darcula Schemes. Google is thus likely to succeed on its Lanham Act claims.

10. *RICO*. Google has shown a likelihood of success on the merits of its claim that Defendants have violated and continue to violate the RICO statute, and that Defendants engaged in a RICO conspiracy.

a. Google has shown that Defendants are active participants in the operation and management of the Darcula Enterprise, which uses Magic Cat 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.

b. Google has established that Defendants constitute an enterprise. Defendants are associated-in-fact and share a common purpose defrauding victims into disclosing sensitive personal information, including financial account details, and stealing their money. Darcula Enterprise members all take part in directing the aspects of the scheme: some develop the Magic Cat software, architecture, and user interface; others manage an online community that recruits new Enterprise members; others supply potential victims' contact information; others specialize in phishing

strategies; and still others steal information and money from victims after the Enterprise phishes their credentials. Defendants collaborate to establish, grow, and manage the Darcula Enterprise, and coordinate to execute sophisticated phishing schemes.

c. Google has established that Defendants have engaged in a pattern of racketeering activity. *See* 18 U.S.C. § 1961(1), (5); *id.* § 2332b(g)(5)(B). The predicate acts include violations of the federal wire fraud statute, 18 U.S.C. § 1343. Defendants have, with intent to defraud and obtain money or property by means of false or fraudulent pretenses, committed wire fraud and continue to commit wire fraud by transmitting signals in interstate or foreign commerce for the purpose of deceiving device owners into submitting sensitive personal or financial information through deception, in violation of 18 U.S.C. § 1343.

d. Google has suffered injury to its business or property as a result of these predicate offenses by devoting substantial financial resources to investigate and remediate Defendants' criminal schemes in order to protect its goodwill and reputation.

e. Google has demonstrated that Defendants have engaged in a RICO conspiracy. The links among the Defendants—such as use of the Magic Cat software, communication over dedicated Telegram channels, and the methods used to deploy phishing schemes using Magic Cat and other Enterprise-controlled resources—demonstrate that the Enterprise formed an agreement as part of a common scheme and conspiracy.

11. *CFAA*. Google has shown a likelihood of success on the merits of its claim that Defendants violated and continue to violate the CFAA. Google has demonstrated that Defendants

have—knowingly and with intent to defraud—trafficked in passwords or similar information through which a computer may be accessed without authorization in interstate commerce through Telegram channels and other online forums in violation of 18 U.S.C. § 1030(a)(6). Defendants transfer and sell phished account credentials and authorization codes to other members of the Enterprise and other cybercriminals. Defendants' actions have caused loss to one or more persons in excess of $5,000 in a one-year period. *See id.* §§ 1030(g), 1030(c)(4)(A)(i)(I), including loss to Google, *see id.* § 1030(e)(11); *see also Saunders Ventures, Inc. v. Salem*, 797 F. App'x 568, 572–73 (2d Cir. 2019).

Balance of Hardships

12. The equities also favor a temporary restraining order. The Darcula Enterprise is defrauding consumers and injuring Google and continues to victimize more people each day. No countervailing factors weigh against a temporary restraining order. There is no legitimate reason why Defendants should be permitted to continue to weaponize Google's branding to defraud the public and commit cybercrimes.

Public Interest

13. Google has shown that the public interest favors granting a temporary restraining order.

14. The Darcula Enterprise has defrauded over one million victims, while using their ill-gotten funds to support other criminal schemes. With each passing day, Defendants deceive new victims. Protection from malicious cyberattacks and other cybercrimes is strongly in the public interest.

15. The public interest is also served by enforcing statutes designed to protect the public, including RICO, the Lanham Act, and the CFAA.

Good Cause for *Ex Parte* Relief

16. As discussed above, Google has set forth facts demonstrating immediate and irreparable harm. There is good cause to believe that if Defendants are provided advance notice of Google's TRO application or this Order, they would dissipate the Darcula Enterprise's infrastructure and resources, allowing them to continue their misconduct, and they would destroy, move, hide, conceal, or otherwise make inaccessible to the Court evidence of their misconduct.

Good Cause for Alternative Service

17. The Court finds good cause exists to grant alternative service of the filings in this matter by email using any information available from web-hosting companies provided in connection with domain names used in the Darcula Schemes and/or any email addresses identified through Google's investigation; website publication; and/or other means because Google establishes that traditional service methods would be futile. Given the online nature of Defendants' conduct, online alternative service is most likely to give Defendants notice of the filings pertaining to this lawsuit.

TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

IT IS HEREBY ORDERED that Defendants, their officers, agents, servants, employees, attorneys, and all others in active concert or participation with them, and each of the foregoing, who receive actual notice of this Order by personal service or otherwise ("Restrained Parties"), are temporarily restrained and enjoined, from, anywhere in the world:

18. Using, linking to, transferring, selling, exercising control over, or otherwise owning any interest in or accessing Magic Cat or the Internet domains through which the Darcula Enterprise perpetrates its phishing schemes, set forth in **Appendix A** to the Naxo Declaration in

Support of Plaintiff's Motion for an *Ex Parte* Temporary Restraining Order and Order to Show Cause ("Appendix A");

19. Attacking and compromising the security of the computers and networks of Google's customers;

20. Intentionally accessing protected computers and computer networks of Google's customers without authorization;

21. Sending messages or advertisements with links to malicious websites;

22. Engaging in phishing schemes;

23. Stealing or selling credentials from victims of phishing schemes;

24. Monitoring the activities of Google or Google's customers or stealing information from them;

25. Impersonating Google, its systems, products, and services;

26. Creating websites that falsely indicate that they are associated with Google, YouTube, or any other Google product or affiliate, through use of Google's trademarks and/or other false and/or misleading representations;

27. Misappropriating that which rightfully belongs to Google, Google's customers and users, or in which Google has a proprietary interest;

28. Configuring, deploying, operating, or otherwise participating in or facilitating the Darcula Enterprise described in the moving papers, including but not limited to the Internet domain names listed in Appendix A and through any other component or element of Defendants' illegal infrastructure in any location, including infrastructure Defendants may attempt to rebuild;

29. Delivering malicious code designed to steal credentials;

30. Selling access to the accounts of Google's customers;

31. Offering, promoting, or selling victims' credit cards or other financial information to others for use;

32. Using, transferring, exercising control over, or accessing any accounts used in the transfer of money or electronic currency, including cryptocurrency, or in the processing of card-based transactions, as a means to further Defendants' unlawful schemes; and/or

33. Undertaking any similar activity that inflicts harm on Google, Google's customers, or the public.

34. Upon service as provided for in this Order, Defendants and other Restrained Parties shall be deemed to have actual notice of the issuance and terms of the Order, and any act by any of the Restrained Parties in violation of any of the terms of the Order may be considered and prosecuted as contempt of court.

35. The Clerk of the Court is to issue a summons to Defendant Doe 1 a/k/a Yucheng Chang and a summons to Defendants Does 2–25 for Google to serve on Defendants.

36. Service of this Order shall be effectuated on or before January 4, 2025.

IT IS FURTHER ORDERED that the Restrained Parties are temporarily restrained and enjoined from:

37. Using and infringing Google's trademarks, including but not limited to Plaintiff's Google mark (RN: 5365541), Google Play mark (RN: 5628029), and YouTube mark (RN: 87984068), and/or other trademarks, trade names, service marks, or Internet domain addresses or names containing or infringing such trademarks, trade names or service marks, as set forth in **Appendix B** to the Google Declaration in Support of Plaintiff's Motion for an *Ex Parte* Temporary Restraining Order and Order to Show Cause, which contains Google's trademarks, trade names, service marks, or Internet domain addresses or names containing or infringing such trademarks,

trade names or service marks, or other intellectual property infringed as a result of Defendants' activities;

38. Using in connection with Defendants' activities, products or services with any false or deceptive designation, representations, or descriptions of Defendants or of their activities, whether by symbols, words, designs, or statements, which would damage or injure Google or its customers or users, or would give Defendants an unfair competitive advantage or result in deception of consumers; and

39. Acting in any other manner that suggests in any way that Defendants' activities, products, or services come from or are somehow sponsored by or affiliated with Google, or passing off Defendants' activities, products, or services as Google's.

IT IS FURTHER ORDERED that, pursuant to the All Writs Act, Google may serve this Order on the persons or entities hosting or providing services related to the domains identified in Appendix A, requesting that those persons and entities take their best efforts to implement the following actions:

40. Take reasonable steps to identify incoming and/or outgoing Internet traffic on their respective networks that originates or is being sent from or to the domains identified in Appendix A;

41. Within three (3) business days of receipt of this Order, or as soon as practicable, take reasonable steps to block and/or disrupt access of incoming and/or outgoing Internet traffic or communications on their respective networks that originates and/or is being sent from or to the domains identified in Appendix A by Defendants or Defendants' representatives or resellers, except as explicitly provided for in this Order;

42. Take other reasonable steps to block and/or disrupt access of such traffic to and/or from any other IP addresses, domains, or Internet channels to which Defendants may move the Darcula infrastructure, including those identified by Google in an amendment to Appendix A, to ensure that Defendants cannot use such infrastructure to facilitate and expand the use of Magic Cat or continue to perpetrate illegal acts;

43. Make the computers, servers, electronic data storage devices, software, data, or media assigned to or otherwise associated with the domains set forth in Appendix A and make them inaccessible from any other computer on the Internet, any internal network, or in any other manner, to Defendants, Defendants' representatives, and all other persons, except as otherwise ordered herein;

44. Completely, and until further order of this Court, suspend all services to Defendants or Defendants' representatives or resellers associated with the domains set forth in Appendix A;

45. Should a provider identify any content and/or software hosted at the domains listed in Appendix A that it reasonably believes is not associated with Defendants, the provider shall preserve any such content and/or software; and contact Google's counsel, Laura Harris, at King & Spalding LLP, 1290 Avenue of the Americas, 14th Floor, New York, New York 10104-0101, and lharris@kslaw.com, within one (1) business day;

46. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives, and refrain from publicizing this Order until the steps required by this Order are executed in full, except as necessary to communicate with hosting companies, data centers, Google, or other ISPs to execute this Order;

47. Not enable, and take all reasonable steps to prevent, any circumvention of this Order by Defendants or Defendants' representatives associated with the domains listed in

Appendix A, including without limitation enabling, facilitating, and/or allowing Defendants or Defendants' representatives or resellers to rent, lease, purchase, or otherwise obtain other services associated with those domains and IP addresses;

48. Preserve, retain, and produce to Google all documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or controlling the domains set forth in Appendix A, including any and all individual or entity names, mailing addresses, e-mail addresses, facsimile numbers, telephone numbers, or similar contact information, including but not limited to such contact information reflected in billing, usage, access, and contact records and all records, documents, and logs associated with the use of or access to such domains and IP addresses;

49. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order; and

50. Completely preserve the computers, servers, electronic data storage devices, software, data, or media assigned to or otherwise associated with the domain names set forth in Appendix A, and preserve all evidence of any kind related to the content, data, software or accounts associated with such domains, IP addresses, and computer hardware.

51. In determining the method and mechanism to disable content and software associated with Defendants, the relevant persons and/or entities shall reasonably confer with Plaintiff's counsel of record in this action.

IT IS FURTHER ORDERED that Google may amend Appendix A if it identifies other domains used by Defendants in connection with the Darcula Enterprise, including any such domains that might not yet exist, without further order of this Court.

IT IS FURTHER ORDERED, that, good cause having been shown, Google may effectuate service using alternative service, including service of process, by electronic means—including by email using any information available from web-hosting companies provided in connection with domain names used in the Darcula Schemes or identified by Google in its investigation; website publication; and/or other means ordered herein—shall be deemed effective as to Defendants through the pendency of this action.

IT IS FURTHER ORDERED, that, good cause having been shown, this Court shall extend the TRO for an additional nine days, until January 9, 2026. Google's request is not the result of any lack of diligence on its part but instead based upon the elaborate nature of Defendants' unlawful conduct and the need to disrupt that conduct over the holidays. Defendants will not be prejudiced by the extension Google seeks. Defendants do not have any legitimate interest that will be impaired by a brief extension of the TRO; they are being enjoined from engaging in conduct that is already prohibited by law.

Security for Temporary Restraining Order

IT IS FURTHER ORDERED that Google shall post bond in the amount of $75,000 to be filed with the Clerk. The Clerk shall accept Google's submission of $75,000 in satisfaction of this Order's bond requirement.

Hearing On Order to Show Cause

IT IS FURTHER ORDERED pursuant to Federal Rule of Civil Procedure 65(b), and good cause having been shown that a brief extension of the TRO is warranted, that Defendants shall appear before this Court on January 9, 2026, at 10:00 am to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against Defendants, enjoining the conduct temporarily restrained by the preceding provisions of this

Order. Good cause has been shown for this Order to remain in effect through the Preliminary Injunction hearing, absent further order from the Court, given the need for additional time to effectuate the disruption ordered herein in light of the upcoming holidays.

So ordered.

United States District Judge

Date: 12/17/25

Time: 6:40 p.m.

Place: New York, NY

Exhibit C

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC,

Plaintiff,

v.

DOE 1 a/k/a YUCHENG CHANG and DOES 2–25,

Defendants.

Civil Action No.: 1:25-cv-10440-JSR

[PROPOSED] PRELIMINARY INJUNCTION ORDER

Plaintiff Google LLC has filed a Complaint for injunctive and other relief to stop Defendants Doe 1 a/k/a Yucheng Chang and Does 2–25, a criminal enterprise (the "Darcula Enterprise" or the "Enterprise"), from using novel software to facilitate large-scale phishing attacks that have harmed over one million victims, including Google.

Google filed a Complaint alleging claims under (1) the Racketeer Influenced and Corrupt Organizations Act ("RICO"), 18 U.S.C. § 1962(c)–(d) (Count I); (2) the Lanham Act, 15 U.S.C. §§ 1114(1), 1125(a)(1)(A), 1125(a)(1)(B) (Count II); and (3) the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a)(6) (Count III). Google moved *ex parte* for a temporary restraining order and an order to show cause why a preliminary injunction should not issue under Federal Rule of Civil Procedure 65 and 28 U.S.C. § 1651.

On December 17, 2025, this Court issued a Temporary Restraining Order ("TRO") and order for Defendants to show cause why a preliminary injunction should not issue.

THE COURT HEREBY FINDS THAT:

1. This Court has federal-question jurisdiction over Google's claims under RICO, the Lanham Act, and the CFAA pursuant to 28 U.S.C. § 1331.

2. This Court has personal jurisdiction over Defendants because:

a. Defendants have intentionally targeted and harmed Google, a company based in the United States. Defendants also have engaged in intentional, wrongful, illegal, and/or tortious acts, the effects of which Defendants intended to and knew would be felt in the United States and New York. Google does business in New York and has done business in New York for many years, including in this District.

b. Defendants have affirmatively directed actions at the United States, including this District, and Defendants attempted to phish and have successfully phished personal and financial information from victims within this District and New York State.

c. Defendants have used Google's trademarks as part of fake websites used to solicit victims' personal and financial information within this District and New York State, and have directed multiple forms of electronic communication to user devices in this District and New York State.

3. Venue is proper in this judicial district under 28 U.S.C. § 1391(c)(3) because Defendants are not residents of the United States and may be sued in any judicial district. Venue is also proper in this judicial district under 28 U.S.C. § 1391(b)(2) and 18 U.S.C. § 1965(a) because a substantial part of the events or omissions giving rise to Google's claims occurred in this judicial district, because a substantial part of the harm caused by Defendants has occurred in this judicial district, and because Defendants transact their affairs in this judicial district. Moreover, Defendants are subject to personal jurisdiction in this judicial district, and no other venue appears to be more appropriate.

4. The Complaint pleads facts with the specificity required by the Federal Rules of Civil Procedure and states claims against Defendants for violations of (1) RICO, 18 U.S.C.

§ 1962(c)–(d) (Count I); (2) the Lanham Act, 15 U.S.C. §§ 1114(1), 1125(a)(1)(A), 1125(a)(1)(B) (Count II); and (3) the CFAA, 18 U.S.C. § 1030(a)(6) (Count III).

Preliminary Injunction Order Factors

5. The Court finds that Google has established each of the factors required for a preliminary injunction: (1) irreparable harm; (2) a likelihood of success on the merits and/or has established a substantial question as to the merits; (3) the balance of hardships tips in Google's favor; and (4) a preliminary injunction serves the public interest. *Benihana, Inc. v. Benihana of Tokyo, LLC,* 784 F.3d 887, 895 (2d Cir. 2015); *see also Sterling v. Deutsche Bank Nat'l Tr. Co. as Trustees for Femit Tr. 2006-FF6*, 368 F. Supp. 3d 723, 727 (S.D.N.Y. 2019) ("The standard[s] for granting a temporary restraining order and a preliminary injunction pursuant to Rule 65 of the Federal Rules of [Civil] Procedure are identical.").

Irreparable Harm

6. Google has established that it will suffer immediate, irreparable harm if this Court denies its request for a preliminary injunction. Google has shown that Defendants—through their operation of the Darcula Enterprise to participate in and carry out numerous criminal phishing scams (the "Darcula Schemes")—have threatened the security of the Internet and are causing ongoing and irreparable harm to Google and the public by using phishing attacks to steal personal and financial information, defrauding unsuspecting targets, impairing Google's reputation and goodwill, and causing Google (and numerous others) unrecoverable financial losses. Until the Darcula Schemes are disrupted, the Enterprise will continue to profit from its unlawful activities at the expense of Google and members of the public.

7. Defendants' conduct is injuring Google's goodwill and damaging its reputation by falsely associating Google with fraud perpetrated by the Darcula Enterprise, and injuries to

goodwill and reputation constitute irreparable harm. Google has suffered and continues to suffer economic losses from the Darcula Schemes because Google has expended (and continues to expend) substantial financial resources into developing strong brand recognition associated with its name, logos, and products, and investigating and combat Darcula Schemes and to identify measures necessary to remediate the harms caused by the Darcula Schemes. These injuries constitute irreparable harm, including because Google has shown a likelihood that Defendants would take steps to avoid complying with any judgment.

Likelihood of Success on the Merits

8. Google has demonstrated that its Complaint presents a substantial question as to each of its claims and that it is likely to succeed on the merits of its claims. *See Sterling v. Deutsche Bank Nat'l Tr. Co. as Trs. for Femit Tr. 2006-FF6*, 368 F. Supp. 3d 723, 727 (S.D.N.Y. 2019).

9. *The Lanham Act.* Google has shown a likelihood of success on the merits of its claims that Defendants violated and continue to violate the Lanham Act. Section 1114 of the Lanham Act prohibits infringement of a registered trademark or service mark. Infringement occurs when a valid, protectable mark is used in commerce and is likely to cause confusion, to cause mistake, or to deceive. 15 U.S.C. § 1114(1); *Virgin Enters. Ltd. v. Nawab*, 335 F.3d 141, 146 (2d Cir. 2003). Defendants violated this provision by exploiting Google's trustworthy, well-known, valid, protectable, and registered Marks on their spoofed websites to deceive consumers. Section 1125(a) prohibits false "designations of origin" that are likely to cause confusion as to the sponsorship 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, *Victorinox AG v. B & F System, Inc.*, 114 F. Supp. 3d 132, 139 (S.D.N.Y. 2015), so Google's section 1125(a)(1)(A) claim is 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) have caused injury to the plaintiff. *Church & Dwight Co. v. SPD Swiss Precision Diagnostics, GmBH*, 843 F.3d 48, 65 (2d Cir. 2016). Google has demonstrated that Defendants deceive Internet users by using Google's Marks on their spoofed websites. Google has shown that the representations are literally false because they are not from or endorsed by Google and that the representations are material because the Defendants' schemes are only successful because their websites appear to be real. The messages bearing Google Marks are placed in interstate commerce on the Internet, and Google has demonstrated injury to its goodwill and through costs to combat the Darcula Schemes. Google is thus likely to succeed on its Lanham Act claims.

10. *RICO*. Google has shown a likelihood of success on the merits of its claim that Defendants have violated and continue to violate the RICO statute, and that Defendants engaged in a RICO conspiracy.

a. Google has shown that Defendants are active participants in the operation and management of the Darcula Enterprise, which uses Magic Cat 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.

b. Google has established that Defendants constitute an enterprise. Defendants are associated-in-fact and share a common purpose defrauding victims into disclosing sensitive personal information, including financial account details, and stealing their money. Darcula Enterprise members all take part in directing the aspects of the scheme: some develop the Magic Cat software, architecture, and user interface; others manage an online community that recruits new Enterprise members; others

supply potential victims' contact information; others specialize in phishing strategies; and still others steal information and money from victims after the Enterprise phishes their credentials. Defendants collaborate to establish, grow, and manage the Darcula Enterprise, and coordinate to execute sophisticated phishing schemes.

c. Google has established that Defendants have engaged in a pattern of racketeering activity. *See* 18 U.S.C. § 1961(1), (5); *id.* § 2332b(g)(5)(B). The predicate acts include violations of the federal wire fraud statute, 18 U.S.C. § 1343. Defendants have, with intent to defraud and obtain money or property by means of false or fraudulent pretenses, committed wire fraud and continue to commit wire fraud by transmitting signals in interstate or foreign commerce for the purpose of deceiving device owners into submitting sensitive personal or financial information through deception, in violation of 18 U.S.C. § 1343.

d. Google has suffered injury to its business or property as a result of these predicate offenses by devoting substantial financial resources to investigate and remediate Defendants' criminal schemes in order to protect its goodwill and reputation.

e. Google has demonstrated that Defendants have engaged in a RICO conspiracy. The links among the Defendants—such as use of the Magic Cat software, communication over dedicated Telegram channels, and the methods used to deploy phishing schemes using Magic Cat and other Enterprise-controlled resources—demonstrate that the Enterprise formed an agreement as part of a common scheme and conspiracy.

11. *CFAA*. Google has shown a likelihood of success on the merits of its claim that Defendants violated and continue to violate the CFAA. Google has demonstrated that Defendants have—knowingly and with intent to defraud—trafficked in passwords or similar information through which a computer may be accessed without authorization in interstate commerce through Telegram channels and other online forums in violation of 18 U.S.C. § 1030(a)(6). Defendants transfer and sell phished account credentials and authorization codes to other members of the Enterprise and other cybercriminals. Defendants' actions have caused loss to one or more persons in excess of $5,000 in a one-year period. *See id.* §§ 1030(g), 1030(c)(4)(A)(i)(I), including loss to Google, *see id.* § 1030(e)(11); *see also Saunders Ventures, Inc. v. Salem*, 797 F. App'x 568, 572–73 (2d Cir. 2019).

Balance of Hardships

12. The equities also favor a preliminary injunction. The Darcula Enterprise is defrauding consumers and injuring Google and continues to victimize more people each day. No countervailing factors weigh against a preliminary injunction. There is no legitimate reason why Defendants should be permitted to continue to weaponize Google's branding to defraud the public and commit cybercrimes.

Public Interest

13. Google has shown that the public interest favors granting a preliminary injunction.

14. The Darcula Enterprise has defrauded over one million victims, while using their ill-gotten funds to support other criminal schemes. With each passing day, Defendants deceive new victims. Protection from malicious cyberattacks and other cybercrimes is strongly in the public interest.

15. The public interest is also served by enforcing statutes designed to protect the public, including RICO, the Lanham Act, and the CFAA.

Good Cause for Alternative Service

16. The Court finds good cause exists to grant alternative service, including service of process, of the filings in this matter by email using any information available from web-hosting companies provided in connection with domain names used in the Darcula Schemes and/or any email addresses identified through Google's investigation; website publication; and/or other means because Google establishes that traditional service methods would be futile. Given the online nature of Defendants' conduct, online alternative service is most likely to give Defendants notice of the filings pertaining to this lawsuit.

PRELIMINARY INJUNCTION ORDER

IT IS HEREBY ORDERED that Defendants, their officers, agents, servants, employees, and attorneys, and all others in active concert or participation with them, and each of the foregoing who receive actual notice of this Order by personal service or otherwise ("Restrained Parties"), are preliminarily restrained and enjoined, from, anywhere in the world:

17. Using, linking to, transferring, selling, exercising control over, or otherwise owning any interest in or accessing Magic Cat or the Internet domains through which the Darcula Enterprise perpetrates its phishing schemes, set forth in **Appendix A** to the Naxo Declaration in Support of Plaintiff's Motion for an *Ex Parte* Temporary Restraining Order and Order to Show Cause ("Appendix A");

18. Attacking and compromising the security of the computers and networks of Google's customers;

19. Intentionally accessing protected computers and computer networks of Google's customers without authorization;

20. Sending messages or advertisements with links to malicious websites;

21. Engaging in phishing schemes;

22. Stealing or selling credentials from victims of phishing schemes;

23. Monitoring the activities of Google or Google's customers or stealing information from them;

24. Impersonating Google, its systems, products, and services;

25. Creating websites that falsely indicate that they are associated with Google, YouTube, or any other Google product or affiliate, through use of Google's trademarks and/or other false and/or misleading representations;

26. Misappropriating that which rightfully belongs to Google, Google's customers and users, or in which Google has a proprietary interest;

27. Configuring, deploying, operating, or otherwise participating in or facilitating the Darcula Enterprise described in the moving papers, including but not limited to the Internet domain names listed in Appendix A and through any other component or element of Defendants' illegal infrastructure in any location, including infrastructure Defendants may attempt to rebuild;

28. Delivering malicious code designed to steal credentials;

29. Selling access to the accounts of Google's customers;

30. Offering, promoting, or selling victims' credit cards or other financial information to others for use;

31. Using, transferring, exercising control over, or accessing any accounts used in the transfer of money or electronic currency, including cryptocurrency, or in the processing of card-based transactions, as a means to further Defendants' unlawful schemes; and/or

32. Undertaking any similar activity that inflicts harm on Google, Google's customers, or the public.

33. Upon service as provided for in this Order, Defendants and other Restrained Parties shall be deemed to have actual notice of the issuance and terms of the Order, and any act by any of the Restrained Parties in violation of any of the terms of the Order may be considered and prosecuted as contempt of court.

34. The Clerk of the Court is to issue a summons to Defendant Doe 1 a/k/a Yucheng Chang and a summons to Defendants Does 2–25 for Google to serve on Defendants.

IT IS FURTHER ORDERED that the Restrained Parties are preliminarily restrained and enjoined, from, anywhere in the world:

35. Using and infringing Google's trademarks, including but not limited to Plaintiff's Google mark (RN: 5365541), Google Play mark (RN: 5628029), and YouTube mark (RN: 87984068), and/or other trademarks, trade names, service marks, or Internet domain addresses or names containing or infringing such trademarks, trade names or service marks, as set forth in **Appendix B** to the Google Declaration in Support of Plaintiff's Motion for an *Ex Parte* Temporary Restraining Order and Order to Show Cause, which contains Google's trademarks, trade names, service marks, or Internet domain addresses or names containing or infringing such trademarks, trade names or service marks, or other intellectual property infringed as a result of Defendants' activities;

36. Using in connection with Defendants' activities, products or services with any false or deceptive designation, representations, or descriptions of Defendants or of their activities, whether by symbols, words, designs, or statements, which would damage or injure Google or its customers or users, or would give Defendants an unfair competitive advantage or result in deception of consumers; and

37. Acting in any other manner that suggests in any way that Defendants' activities, products, or services come from or are somehow sponsored by or affiliated with Google, or passing off Defendants' activities, products, or services as Google's.

IT IS FURTHER ORDERED that, pursuant to the All Writs Act, Google may serve this Order on the persons or entities hosting or providing services related to the domains identified in Appendix A, requesting that those persons and entities take their best efforts to implement the following actions:

38. Take reasonable steps to identify incoming and/or outgoing Internet traffic on their respective networks that originates or is being sent from or to the domains identified in Appendix A;

39. Within three (3) business days of receipt of this Order, or as soon as practicable, take reasonable steps to block and/or disrupt access of incoming and/or outgoing Internet traffic or communications on their respective networks that originates and/or is being sent from or to the domains identified in Appendix A by Defendants or Defendants' representatives or resellers, except as explicitly provided for in this Order;

40. Take other reasonable steps to block and/or disrupt access of such traffic to and/or from any other IP addresses, domains, or Internet channels to which Defendants may move the Darcula infrastructure, including those identified by Google in an amendment to Appendix A, to

ensure that Defendants cannot use such infrastructure to facilitate and expand the use of Magic Cat or continue to perpetrate illegal acts;

41. Make the computers, servers, electronic data storage devices, software, data, or media assigned to or otherwise associated with the domains set forth in Appendix A and make them inaccessible from any other computer on the Internet, any internal network, or in any other manner, to Defendants, Defendants' representatives, and all other persons, except as otherwise ordered herein;

42. Completely, and until further order of this Court, suspend all services to Defendants or Defendants' representatives or resellers associated with the domains set forth in Appendix A;

43. Should a provider identify any content and/or software hosted at the domains listed in Appendix A that it reasonably believes is not associated with Defendants, the provider shall preserve any such content and/or software; and contact Google's counsel, Laura Harris, at King & Spalding LLP, 1290 Avenue of the Americas, 14th Floor, New York, New York 10104-0101, and lharris@kslaw.com, within one (1) business day;

44. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives, and refrain from publicizing this Order until the steps required by this Order are executed in full, except as necessary to communicate with hosting companies, data centers, Google, or other ISPs to execute this Order;

45. Not enable, and take all reasonable steps to prevent, any circumvention of this Order by Defendants or Defendants' representatives associated with the domains listed in Appendix A, including without limitation enabling, facilitating, and/or allowing Defendants or Defendants' representatives or resellers to rent, lease, purchase, or otherwise obtain other services associated with those domains and IP addresses;

46. Preserve, retain, and produce to Google all documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or controlling the domains set forth in Appendix A, including any and all individual or entity names, mailing addresses, e-mail addresses, facsimile numbers, telephone numbers, or similar contact information, including but not limited to such contact information reflected in billing, usage, access, and contact records and all records, documents, and logs associated with the use of or access to such domains and IP addresses;

47. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order; and

48. Completely preserve the computers, servers, electronic data storage devices, software, data, or media assigned to or otherwise associated with the domain names set forth in Appendix A, and preserve all evidence of any kind related to the content, data, software or accounts associated with such domains, IP addresses, and computer hardware.

49. In determining the method and mechanism to disable content and software associated with Defendants, the relevant persons and/or entities shall reasonably confer with Plaintiff's counsel of record in this action.

IT IS FURTHER ORDERED that Google may amend Appendix A if it identifies other domains used by Defendants in connection with the Darcula Enterprise, including any such domains that might not yet exist, without further order of this Court.

IT IS FURTHER ORDERED that, because sufficient cause has been shown, alternative service, including service of process, by electronic means—including by email using any information available from web-hosting companies provided in connection with domain names used in the Darcula Schemes or identified by Google in its investigation; website publication;

and/or other means ordered herein—shall be deemed effective as to Defendants through the pendency of this action.

Security for Preliminary Injunction Order

IT IS FURTHER ORDERED that Google's submission of the $75,000 bond to the Clerk satisfied the requirements of this Court's TRO. No additional bond is necessary.

So ordered.

United States District Judge

Date: 2/9/26

Time: 9:10 a.m.

Exhibit D

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC, Plaintiff, -v- DOE 1 a/k/a YUCHENG CHANG and DOES 2-25, Defendants.	25-cv-10440 (JSR) MEMORANDUM ORDER

JED S. RAKOFF, U.S.D.J.:

Contemporaneous with this Order, the Court grants plaintiff Google LLC's ("Google") unopposed preliminary injunction motion. The Court writes separately to address the issue of service.

On December 17, 2025, plaintiff filed this action against twenty-five "Doe" defendants, who plaintiff contends are likely located in China. Plaintiff also sought a TRO from this Court and requested the Court's permission to serve defendants by alternative means, namely by website publication and email under Federal Rule of Civil Procedure 4(f)(3). See Pl's Mem. of Law in Support of its Mtn. for an Ex Parte TRO ("TRO Mem.") at 23, ECF No. 8. The Court granted the TRO and authorized the alternative means of service requested. See ECF No. 18.

The next day, the Second Circuit held in Smart Study Co. v. Shenzhenshixindajixieyouxiangongsi, No. 24-313, 2025 WL 3672740 (2d Cir. Dec. 18, 2025), that the Hague Convention, where it applies, does not permit email service of defendants located abroad. Accordingly,

at the January 9, 2026 preliminary injunction hearing, the Court directed plaintiff to submit supplemental briefing addressing the impact, if any, of the Second Circuit's decision in Smart Study on the means of service appropriate in this action.

Having considered plaintiff's supplemental briefing, the Court concludes that alternative service by electronic means is proper and is not prohibited by the Hague Convention in this case. The Hague Convention, which generally governs service of individuals located abroad, does not apply "where the address of the person to be served with the document is not known." Hague Convention, Art. I; see also Smart Study, 2025 WL 3672740, at *2. Courts in this district and elsewhere have concluded that an address is "not known" "if the plaintiff exercised reasonable diligence in attempting to discover a physical address for service of process and was unsuccessful in doing so." Kelly Toys Holdings, LLC v. Top Dep't Store, 22 Civ. 558 (PAE), 2022 WL 3701216, at *6 (S.D.N.Y. Aug. 26, 2022) (citation omitted) (collecting cases). The exercise of reasonable diligence is a fact-specific inquiry, but Courts have found it satisfied when a plaintiff had attempted to obtain the defendant's address in a variety of ways. See Kumar v. Alhunaif, 2023 WL 8527671, at *3 (S.D.N.Y. Dec. 8, 2023).

Plaintiff has demonstrated reasonable diligence in this case. Plaintiff has attempted to ascertain defendants' addresses through multiple means, 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 addresses obtained. See Pl.'s Suppl. Br. at 9-10, ECF No. 27. As set forth in plaintiff's detailed declarations and in its supplemental brief, plaintiff has been unable to verify the true identities of the defendants or their physical addresses, and, of the addresses obtained from domain registrars, plaintiff's further investigations have determined that the addresses are either fake, lacking necessary information, associated with different entities, and/or are located in countries that are not signatories to the Hague Convention. See id. at 10-11; Harris Decl. ¶¶ 7, 17, 19-26, ECF No. 28; Cai Decl. ¶¶ 6, 9, ECF No. 30; Lam Decl. ¶¶ 5, 1,7 ECF No. 29. Accordingly, because defendants' addresses are "not known," the Hague Convention does not apply to prohibit email service in this case.

In the absence of any prohibition under the Hague Convention, the Court concludes that service through email and website publication is proper under Federal Rule of Civil Procedure 4(f)(3). See Fed. R. Civ. P. 4(f)(3) (authorizing service "by other means not prohibited by international agreement, as the court orders"); see also Smart Study, 2025 WL 3672740, at *2 (noting that "[b]oth the Rule 4(f)(2) and 4(f)(3) paths are open when" the defendant's address is unknown). Indeed, as plaintiff explains, the email addresses that plaintiff has obtained from domain registrars for domains associated with defendants are likely valid and operational given that domain registrars use those addresses for billing and other administrative issues and because defendants' enterprise relies on the use of those domains. See Harris

Decl. ¶ 14. Thus, plaintiff has "supplied the Court with some facts indicating that the person to be served would be likely to receive the summons and complaint at the given email address." NYKCool A.B. v. Pac. Int'l Servs., Inc., 66 F. Supp. 3d 385, 391 (S.D.N.Y. 2014). Accordingly, the alternative means of service that plaintiff proposes is "reasonably calculated, under all the circumstances, to apprise [defendants] of the pendency of the action." See Kelly Toys, 2022 WL 3701216, at *9 (quoting Advanced Access Content Sys. Licensing Adm'r, LLC v. Shen, No. 12-CV-1112 (VSB), at *5 (S.D.N.Y. Sept. 30, 2018).

The Court therefore grants plaintiff's request to serve defendants by the alternative means specified.

SO ORDERED.

New York, NY
February 9, 2026

JED S. RAKOFF, U.S.D.J.

Exhibit E

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC, *Plaintiff,* v. DOE 1 a/k/a YUCHENG CHANG and DOES 2–25, *Defendants.*	Civil Action No.: 1:25-cv-10440-JSR

Plaintiff Google LLC ("Google") has sued Defendants Does 1-25 associated with the Internet domains listed in the pleading set forth below. Google alleges that Defendants have deployed a phishing-as-as-service model to facilitate and execute phishing attacks designed to steal personal and financial information, and Defendants have misused Google trademarks in their scheme. Google alleges that, through these actions, the Defendants have violated federal law. Google sought and received a temporary restraining order enjoining the Defendants from these and other activities and directing the third parties associated with Defendants' Internet domains to take all steps necessary to disable access to and operation of Magic Cat/Darcula-associated domains. Google intends to seek a preliminary injunction and other equitable relief. Full copies of the complaint, related filings, and orders from the Court are available below.

NOTICE TO DEFENDANT: READ THESE PAPERS CAREFULLY! A hearing to show cause why the Court should not enter a Preliminary Injunction will be held on January 9, 2026 at 10 a.m.

You must "appear" in this case or the other side will win automatically. To "appear" you must file with the court a legal document called a "motion" or "answer." The "motion" or "answer" must be given to the court clerk or administrator within 21 days of the date of first publication specified herein. It must be in proper form and have proof of service on Google's attorney, Laura Harris, King & Spalding LLP, 1290 Avenue of the Americas, 14th Fl., New York, NY 10104-0101. If you have questions, you should consult with your own attorney immediately.

Complaint and Summons

Complaint

Summons

Court Orders

Order Granting Temporary Restraining Order

Order Granting Motion to Seal

Preliminary Injunction Order

Order regarding Alternative Service

Order Unsealing Appendix A

Application for Temporary Restraining Order and Preliminary Injunction

Motion for Temporary Restraining Order

Memorandum of Law in Support of Temporary Restraining Order and Order to Show Cause

[Proposed] Temporary Restraining Order and Order to Show Cause

Declaration in Support of Plaintiff's Motion for Temporary Restraining Order (L. Harris)

Declaration in Support of Plaintiff's Motion for Temporary Restraining Order (Google)

Declaration in Support of Plaintiff's Motion for Temporary Restraining Order (NAXO)

Appendix A

Motion to Seal Appendix A & Redact Certain Information

Motion to File Appendix A under Seal and Redact Certain Identifying Information

Memorandum of Law in Support of Motion to File Appendix A under Seal and Redact Certain Identifying Information

[Proposed] Order Granting Plaintiff's Motion to File Appendix A under Seal and Redact Certain Identifying Information

January 9, 2026 Hearing

Plaintiff's Supplemental Memorandum of Law

Declaration in Support of Plaintiff's Supplemental Memorandum of Law (L. Harris)

Exhibit 1 to Declaration in Support of Plaintiff's Supplemental Memorandum of Law (L. Harris)

Declaration in Support of Plaintiff's Supplemental Memorandum of Law (R. Cai)

Declaration in Support of Plaintiff's Supplemental Memorandum of Law (L. Wing)

Service Related Pleadings and Third Party Filings

Certificate of Service (January 8, 2026)

Contact us:

If you wish to contact us, please use the contact information below:

Laura Harris
KING & SPALDING LLP
1290 Avenue of the Americas
14th Floor
New York, NY 10104
Phone: +1 (212) 556-2100
lharris@kslaw.com

Christine Carletta
KING & SPALDING LLP
1700 Pennsylvania Ave., NW
2nd Floor
Washington, DC 20006
Phone: +1 (202) 626-5591
ccarletta@kslaw.com

Exhibit F

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC, *Plaintiff*, v. DOES 1–25, *Defendants.*	Civil Action No. 1:25-cv-10440-JSR

CERTIFICATE OF SERVICE

I, Laura Harris, counsel for Google LLC ("Google") in this action, declare under penalty of perjury that the following is true and correct to the best of my knowledge:

1. I am a partner with the law firm of King & Spalding LLP, and I oversaw Google's efforts to provide service and notice to Defendants by email and website publication, as authorized by the Court's *Ex Parte* Temporary Restraining Order and Order to Show Cause (the "Order"), entered December 17, 2025.

2. On December 17, 2025, I caused notice of the Order to be sent to the registrars identified in Appendix A to the Order requesting, in part, that those third parties provide contact information associated with the domains identified in Appendix A.

3. On January 4, 2026, King & Spalding LLP served Defendants by email, using the email addresses identified in Google's investigation or that registrars had provided to date, and by website publication with copies of the following documents:

   a. Complaint, dated December 17, 2025;

   b. The Order, dated December 17, 2025;

   c. Plaintiff's Motion for an *Ex Parte* Temporary Restraining Order and Order to Show Cause, dated December 17, 2025;

d. Plaintiff's Memorandum of Law in Support of Its Motion for an *Ex Parte* Temporary Restraining Order and Order to Show Cause, dated December 17, 2025;

e. [Proposed] *Ex Parte* Temporary Restraining Order and Order to Show Cause, dated December 17, 2025;

f. Declaration of Laura Harris in Support of Plaintiff's Motion for an *Ex Parte* Temporary Restraining Order and Order to Show Cause, dated December 17, 2025;

g. Google Declaration in Support of Plaintiff's Motion for an *Ex Parte* Temporary Restraining Order and Order to Show Cause, dated December 17, 2025;

h. Naxo Declaration in Support of Plaintiff's Motion for an *Ex Parte* Temporary Restraining Order and Order to Show Cause, dated December 17, 2025;

i. Plaintiff's Motion to File Appendix A Under Seal and Redact Certain Identifying Information, dated December 17, 2025;

j. Plaintiff's Memorandum of Law in Support of Its Motion to Redact Certain Personal Identifying Information and File Appendix A Under Seal, dated December 17, 2025;

k. [Proposed] Order Granting Plaintiff's Motion to File Appendix A Under Seal and Redact Certain Identifying Information, dated December 17, 2025; and

l. Order Granting Plaintiff's Motion to Redact Certain Personal Identifying Information and to File Appendix A under Seal.

Executed on January 8, 2026, in New York, New York.

/s/ Laura Harris
Laura Harris

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC, *Plaintiff*, v. DOE 1 a/k/a YUCHENG CHANG and DOES 2–25, *Defendants*.	Civil Action No. 1:25-cv-10440-JSR

CERTIFICATE OF SERVICE

I, Grace Miller, counsel for Google LLC ("Google") in this action, declare under penalty of perjury that the following is true and correct to the best of my knowledge:

1. I am an associate with the law firm of King & Spalding LLP, and I oversaw Google's efforts to provide service and notice to Defendants by email and website publication, as authorized by the Court's *Ex Parte* Temporary Restraining Order and Order to Show Cause, issued December 17, 2025, ECF No. 18, the Court's Preliminary Injunction Order, issued February 9, 2026, ECF No. 34, and the Court's Memorandum Order issued February 9, 2026, ECF No. 33.

2. On February 9, 2026, King & Spalding LLP served Defendants by email, using the email addresses identified in Google's investigation or that registrars had provided to date, and by website publication with a copy of the Preliminary Injunction Order, issued February 9, 2026.

3. On February 19, 2026, King & Spalding LLP served Defendants by email and by website publication with copies of the following additional documents:

   a. Certificate of Service, dated January 8, 2026;

   b. Order, issued January 8, 2026;

c. Google's Supplemental Memorandum of Law in Response to January 9, 2026 Hearing, dated January 23, 2026;

d. Declaration of Laura Harris in Support of Google's Supplemental Memorandum of Law in Response to January 9, 2026 Hearing, dated January 23, 2026

e. Declaration of Lam Sze Wing in Support of Google's Supplemental Memorandum of Law in Response to January 9, 2026 Hearing, dated January 23, 2026;

f. Declaration of Ron (Rongwei) Cai in Support of Google's Supplemental Memorandum of Law in Response to January 9, 2026 Hearing, dated January 23, 2026;

g. Memorandum Order, dated February 9, 2026; and

h. Summons in a Civil Action, issued February 19, 2026.

Executed on February 26, 2026, in New York, New York.

/s/ Grace Miller
Grace Miller

Exhibit 10

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----------X

Google LLC

Plaintiff(s),

- against -

Doe 1 a/k/a Yucheng Chang and Does 2–25

Defendant(s),

----------X

1:25 Civ. 10440 (JSR)

CLERK'S CERTIFICATE OF DEFAULT

I, TAMMI M. HELLWIG, Clerk of the United States District Court for the Southern District of New York, do hereby certify that this action was commenced on Dec. 17, 2025 **with the filing of a summons and complaint, a copy of the summons and complaint was served on defendant(s)** Doe 1 a/k/a Yucheng Chang and Does 2–25 **by personally serving** the Defendants in the manner ordered by the Court on Dec. 17, 2025, ***and proof of service was therefore filed on*** 1/8/2026, 2/19/26, ***Doc. #(s)*** 22, 35.

I further certify that the docket entries indicate that the defendant(s) has not filed an answer or otherwise moved with respect to the complaint herein. The default of the defendant(s) is/are hereby noted.

Dated: New York, New York

March 16, 2026

TAMMI M. HELLWIG
Clerk of Court

By: Nazam Dulal
Deputy Clerk

Exhibit 11

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC, *Plaintiff,* v. DOE 1 a/k/a YUCHENG CHANG and DOES 2–25, *Defendants.*	Civil Action No.: 1:25-cv-10440-JSR

Plaintiff Google LLC ("Google") has sued Defendants Does 1-25 associated with the Internet domains listed in the pleading set forth below. Google alleges that Defendants have deployed a phishing-as-as-service model to facilitate and execute phishing attacks designed to steal personal and financial information, and Defendants have misused Google trademarks in their scheme. Google alleges that, through these actions, the Defendants have violated federal law. Google sought and received a temporary restraining order enjoining the Defendants from these and other activities and directing the third parties associated with Defendants' Internet domains to take all steps necessary to disable access to and operation of Magic Cat/Darcula-associated domains. Google intends to seek a preliminary injunction and other equitable relief. Full copies of the complaint, related filings, and orders from the Court are available below.

NOTICE TO DEFENDANT: READ THESE PAPERS CAREFULLY! A hearing to show cause why the Court should not enter a Preliminary Injunction will be held on January 9, 2026 at 10 a.m.

You must "appear" in this case or the other side will win automatically. To "appear" you must file with the court a legal document called a "motion" or "answer." The "motion" or "answer" must be given to the court clerk or administrator within 21 days of the date of first publication specified herein. It must be in proper form and have proof of service on Google's attorney, Laura Harris, King & Spalding LLP, 1290 Avenue of the Americas, 14th Fl., New York, NY 10104-0101. If you have questions, you should consult with your own attorney immediately.

Complaint and Summons

Complaint

Summons

Court Orders

Order Granting Temporary Restraining Order

Order Granting Motion to Seal

Preliminary Injunction Order

Order regarding Alternative Service

Order Unsealing Appendix A

Application for Temporary Restraining Order and Preliminary Injunction

Motion for Temporary Restraining Order

Memorandum of Law in Support of Temporary Restraining Order and Order to Show Cause

[Proposed] Temporary Restraining Order and Order to Show Cause

Declaration in Support of Plaintiff's Motion for Temporary Restraining Order (L. Harris)

Declaration in Support of Plaintiff's Motion for Temporary Restraining Order (Google)

Declaration in Support of Plaintiff's Motion for Temporary Restraining Order (NAXO)

Appendix A

Motion to Seal Appendix A & Redact Certain Information

Motion to File Appendix A under Seal and Redact Certain Identifying Information

Memorandum of Law in Support of Motion to File Appendix A under Seal and Redact Certain Identifying Information

[Proposed] Order Granting Plaintiff's Motion to File Appendix A under Seal and Redact Certain Identifying Information

January 9, 2026 Hearing

Plaintiff's Supplemental Memorandum of Law

Declaration in Support of Plaintiff's Supplemental Memorandum of Law (L. Harris)

Exhibit 1 to Declaration in Support of Plaintiff's Supplemental Memorandum of Law (L. Harris)

Declaration in Support of Plaintiff's Supplemental Memorandum of Law (R. Cai)

Declaration in Support of Plaintiff's Supplemental Memorandum of Law (L. Wing)

Service Related Pleadings and Third Party Filings

Certificate of Service (January 8, 2026)

Contact us:

If you wish to contact us, please use the contact information below:

Laura Harris
KING & SPALDING LLP
1290 Avenue of the Americas
14th Floor
New York, NY 10104
Phone: +1 (212) 556-2100
lharris@kslaw.com

Christine Carletta
KING & SPALDING LLP
1700 Pennsylvania Ave., NW
2nd Floor
Washington, DC 20006
Phone: +1 (202) 626-5591
ccarletta@kslaw.com