JUDGE OETKEN

25 CV 04503

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

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

GOOGLE LLC'S MEMORANDUM OF LAW IN SUPPORT OF ITS MOTION FOR *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

FTC v. Pricewert LLC,
No. 5:09-cv-2407-RMW (N.D. Cal. June 2, 2009), ECF No. 12 22

FTC v. Verity Int'l, Ltd.,
2000 WL 1805688 (S.D.N.Y. Dec. 8, 2000) 19

Google LLC v. Starovikov,
2021 WL 6754263 (S.D.N.Y. Dec. 16, 2021) .... *passim*

Google LLC v. Starovikov,
No. 1:21-cv-10260-DLC (S.D.N.Y. Dec. 7, 2021), ECF No. 8 22

Granny Goose Foods, Inc.
v. Bhd. of Teamsters & Auto Truck Drivers Loc. No. 70,
415 U.S. 423 (1974) 21, 22

Hinterberger v. Catholic Health Sys., Inc.,
536 F. App'x 14 (2d Cir. 2013) 15

Juicero, Inc. v. Itaste Co.,
2017 WL 3996196 (N.D. Cal. June 5, 2017) 23

Makekau v. Hawaii,
943 F.3d 1200 (9th Cir. 2019) 24

Microsoft Corp. v. Does 1–18,
2014 WL 1338677 (E.D. Va. Apr. 2, 2014) 14, 23, 25

Microsoft Corp. v. Does 1–2,
2016 WL 9334654 (E.D. Va. Aug. 12, 2016) 2, 9

Microsoft Corp. v. Does 1–2,
2021 WL 4260665 (E.D.N.Y. Sept. 20, 2021) 15, 26

Microsoft Corp. v. Does 1–2,
2021 WL 8444748 (E.D. Va. Aug. 12, 2021) 19

Microsoft Corp. v. Does 1–2,
2024 WL 1708328 (E.D. Va. Jan. 10, 2024) 19

Microsoft Corp. v. Does 1–51,
2017 WL 10087886 (N.D. Ga. Nov. 17, 2017) 9, 25

Microsoft Corp. v. Does 1–51,
2018 WL 3471083 (N.D. Ga. June 18, 2018) 15

Microsoft Corp. v. Does 1–8,
2014 WL 12575722 (E.D. Va. June 27, 2014) 9

Microsoft Corp. v. Does 1–8,
2015 WL 4937441 (E.D. Va. Aug. 17, 2015)..11

Microsoft Corp. v. Does 1–82,
2013 WL 2632612 (W.D.N.C. June 10, 2013)..9

Microsoft Corp. v. Does 1–82,
2013 WL 6119242 (W.D.N.C. Nov. 21, 2013) 25

Physicians Interactive v. Lathian Sys., Inc.,
2003 WL 23018270 (E.D. Va. Dec. 5, 2003)..15

Register.com, Inc. v. Verio, Inc.,
356 F.3d 393 (2d Cir. 2004) 11

Reves v. Ernst & Young,
507 U.S. 170 (1993)...16

Rio Props., Inc. v. Rio Int'l Interlink,
284 F.3d 1007 (9th Cir. 2002) 23

Saunders Ventures, Inc. v. Salem,
797 F. App'x 568 (2d Cir. 2019)..14

Sophos Ltd. v. Does 1–2,
2020 WL 4722425 (E.D. Va. May 1, 2020) 22

Spool v. World Child Int'l Adoption Agency,
520 F.3d 178 (2d Cir. 2008) 17

Sprint Spectrum L.P. v. Mills,
283 F.3d 404 (2d Cir. 2002) 24

State Farm Mut. Auto. Ins. Co. v. Tri-Borough NY Med. Prac. P.C.,
120 F.4th 59 (2d Cir. 2024) 15

Strougo v. Barclays PLC,
194 F. Supp. 3d 230 (S.D.N.Y. 2016) 9

Suber v. VVP Servs.,
2021 WL 1101235 (S.D.N.Y. Mar. 23, 2021)..19

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 (9th Cir. 1980) 25

United Spinal Ass'n v. Bd. of Elections in City of N.Y.,
2017 WL 8683672 (S.D.N.Y. Oct. 11, 2017)..24

Statutes

Rules

Other Authorities

INTRODUCTION

This is an application for an emergency *ex parte* temporary restraining order to stop a far-reaching criminal enterprise that has silently infiltrated over ten million internet-connected devices around the world and leveraged those devices to commit a wide range of cybercrimes. Defendants are global cybercriminals who surreptitiously preinstall malware in internet-connected devices and trick users into downloading free applications ("apps") that contain malware, granting Defendants and other threat actors access to the devices without the user ever knowing it. This network of malware-infected devices, known as a "botnet," constitutes the largest botnet of personal TV streaming boxes ever discovered, and includes tablets, projectors, and other devices as well. The computing power Defendants control presents a cyber threat that requires immediate intervention to prevent further harm.

Defendants work together to grow, control, and profit from the botnet—known as the BadBox 2.0 botnet—as part of a sophisticated criminal enterprise (the "BadBox 2.0 Enterprise" or the "Enterprise") that targets new victims and infects their devices with malware that enlists the devices in the botnet, thereby increasing the botnet's computing power each day. The Enterprise uses its illicit access to devices in the botnet to commit a range of cybercrimes, including sophisticated ad fraud schemes, and selling access to the devices to other cybercriminals (the "BadBox 2.0 Scheme"). The Enterprise represents a modern, technological incarnation of organized crime. It has already harmed millions of victims around the world, including in New York, and, absent the relief Google seeks here, will continue to harm Google, device users, and the public.

This Court should grant Google's motion and issue the proposed temporary restraining order and order to show cause for a preliminary injunction. The injunction is necessary for Google to carry out its disruption plan to disable the domains, IP addresses, and servers that compose

BadBox 2.0. This Court and others have authorized injunctions to disrupt similar cybercriminal enterprises. *See, e.g.*, *Google LLC v. Starovikov*, 2021 WL 6754263, at *1 (S.D.N.Y. Dec. 16, 2021); *Microsoft Corp. v. Does 1–2*, 2016 WL 9334654, at *1 (E.D. Va. Aug. 12, 2016). These steps will disrupt the Enterprise's control of the botnet and its ability to sell access to victims' devices, thwart the Enterprise's harmful, fraudulent schemes, and impede any further criminal activities by disabling the Enterprise's communication with infected devices.

Google's application establishes the factors necessary to obtain a temporary restraining order and preliminary injunction: irreparable harm, a likelihood of success on the merits, a balance of equities tipping in its favor, and the requested relief is in the public interest. *Daileader v. Certain Underwriters at Lloyds London Syndicate 1861*, 96 F.4th 351, 356 (2d Cir. 2024). At a minimum, even if the Court cannot determine with certainty that Google is more likely than not to prevail on the merits of its claims, injunctive relief is still appropriate because Google's application establishes that there are "sufficiently serious questions going to the merits to make them a fair ground for litigation" and that "the balance of hardships tips decidedly" in Google's favor. *C.D.S. Inc. v. Bradley Zetler, CDS, LLC*, 691 F. App'x 33, 35 (2d Cir. 2017) (internal quotations omitted).

Finally, to prevent irreparable harm, relief must be *ex parte*. First, the harm is ongoing, as the Enterprise exploits and expands its botnet with every passing day. Second, notice would only give the Enterprise the opportunity to avoid the disruption of its schemes by relocating the infrastructure it uses to control the botnet. If this Court grants preliminary relief, Google will provide the Enterprise with notice five days before a hearing on a preliminary injunction or within such time as the Court may order, through service as requested in this motion.

BACKGROUND

Defendants Does 1–25, the Enterprise, are cybercriminals and co-conspirators who operate a modern-day organized crime syndicate. Plaintiff Google's Complaint ("Compl.") ¶ 1;

[redacted], dated May 27, 2025 ("Decl.") ¶ 4. The Enterprise deploys malware onto connected TVs and other devices. Compl. ¶ 2; Decl. ¶¶ 42–46. Once the malware is activated, these devices become part of the BadBox 2.0 botnet—a metastasizing network that the Enterprise uses to carry out illicit schemes without detection by the device user. Compl. ¶ 2; Decl. ¶¶ 24–28, 47–48. Google has undertaken significant efforts to investigate and disrupt BadBox 2.0, but the botnet continues to grow. Decl. ¶¶ 4, 101. As of April 2025, the BadBox 2.0 malware has infected more than ten million devices worldwide, including approximately 170,000 devices in New York and 65,000 in the Southern District of New York alone, and the number of infected devices increases each day. Compl. ¶¶ 15, 93; Decl. ¶¶ 4, 36.

A. The BadBox 2.0 Botnet

A botnet is a network of devices infected by viruses or other malware and controlled by criminals who direct its operations from afar. Compl. ¶¶ 32–36; Decl. ¶ 23. Botnets provide strength in numbers by marshalling the computer power of numerous devices for a common—often criminal—purpose. Compl. ¶ 37; Decl. ¶ 29. Cybercriminals use one or more "command-and-control" servers ("C2 Servers") to direct the devices that make up the botnet. Compl. ¶ 36; Decl. ¶¶ 23, 26.

The Enterprise infects devices that run on a modified version of the Android Open Source Project ("AOSP"). These devices do not have Google Play Protect security features, which are included on devices that use Google's proprietary Android operating system. Compl. ¶ 40; Decl. ¶ 34. The BadBox 2.0 botnet is composed of devices that the Enterprise infected with malware through at least two different methods. Compl. ¶ 47; Decl. ¶ 42. In some cases, the Enterprise pre-installs a "backdoor" (i.e. access point) onto the devices prior to the end user receiving the device. Compl. ¶ 48; Decl. ¶¶ 43–44. When the user turns on the infected device, it is programmed to connect to an Enterprise-controlled C2 Server, which instructs the device to download the malware that establishes the BadBox 2.0 Enterprise's continued control over it. Compl. ¶¶ 48; Decl. ¶¶ 47–48. In other cases, the BadBox 2.0 Enterprise induces users into downloading the backdoor malware onto their devices by creating malicious apps that appear identical to benign versions of the same app. Compl. ¶ 49; Decl. ¶ 46. These malicious apps may, to some extent, function in a similar way to the benign versions of the app that appear in common app stores, which often prevents the user from realizing that the app is malicious. Compl. ¶ 49; Decl. ¶ 46. When the user downloads the infected app—typically, from an unofficial store that does not screen for malware—the malware connects the device to a C2 Server. Compl. ¶¶ 49–50; Decl. ¶¶ 46–48.

Because infected devices may appear to act normally, users typically are unaware that their devices are being controlled behind the scenes. Compl. ¶ 34; Decl. ¶¶ 28, 55, 73, 81. But with each new device that is infected, the botnet's computing power grows. Compl. ¶ 37; Decl. ¶ 29. Consequently, bot controllers can, in a relatively short amount of time, amass an astonishing amount of computing power to support their criminal schemes. Compl. ¶ 37; Decl. ¶ 29.

B. The BadBox 2.0 Criminal Enterprise

Due to the surreptitious nature of the Enterprise's cybercrime, the precise identities of the individuals participating in the BadBox 2.0 Enterprise are unknown. Decl. ¶ 41. But Google and other cybersecurity experts investigating the BadBox 2.0 Enterprise have identified several threat groups that are managing and participating in the Enterprise. Compl. ¶ 12; Decl. ¶ 37. These threat groups develop and use the BadBox 2.0 infrastructure in distinct yet interrelated ways to carry out the Enterprise's schemes. Compl. ¶¶ 41–45; Decl. ¶¶ 37–40. Acting together, the threat actor groups develop and direct the Enterprise's criminal schemes through the infected devices and websites they control. Compl. ¶¶ 41–45; Decl. ¶¶ 37–40.

C. The BadBox 2.0 Enterprise's Criminal Schemes

The Enterprise uses the botnet to carry out multiple criminal schemes, including selling proxy connections to infected devices to perpetrate downstream attacks and at least three types of ad fraud. Compl. ¶ 50.

Sale of Proxy Connections. The BadBox 2.0 Enterprise sells unauthorized access to victims' infected devices. Compl. ¶¶ 52–58; Decl. ¶ 51. Cybercriminals pay for the ability to use infected devices' IP addresses as "residential proxies" to conceal their web traffic and other activities. Compl. ¶ 52; Decl. ¶ 51. Using a "proxy" gives the appearance that the owner of the infected device is engaging in an activity, when instead it is the person remotely accessing the device. Compl. ¶ 54; Decl. ¶ 54. Once the threat actor has access to a proxy, he can commit a wide variety of cyberattacks while concealing his location. Compl. ¶ 56; Decl. ¶ 56. Using the proxy, he can steal information from the infected computer or other networks, steal passwords, take over accounts, create fake accounts, commit ad fraud, "web-scrape" to obtain user data, conduct a "scalping attack" to buy sought-after products to sell them at a higher price, distribute more malware to commit other types of crime or to connect the bot to other C2 servers, or conduct distributed denial-of-service ("DDoS") attacks to make websites, servers, or other resources unusable by flooding them with traffic. Compl. ¶ 56; Decl. ¶ 56.

Ad Fraud. The Enterprise also uses BadBox 2.0 devices to engage in a wide variety of ad fraud schemes. Compl. ¶ 59; Decl. ¶ 60. As a general matter, ad fraud occurs when a scammer intentionally manipulates online advertising programs. Compl. ¶ 59; Decl. ¶ 60. They generate fake clicks, views, or downloads and trick advertisers and ad networks into paying them for advertising that ultimately is not viewed by a real person. Compl. ¶ 59; Decl. ¶ 60. The Enterprise uses the botnet to commit ad fraud on Google's Ad Network in at least three ways. Compl. ¶ 68; Decl. ¶ 72.

First, the Enterprise uses apps to request and render hidden ads. Compl. ¶¶ 69–77; Decl. ¶¶ 73–80. In this scheme, members of the BadBox 2.0 Enterprise preinstall home-screen launcher apps onto infected devices. Compl. ¶ 69; Decl. ¶ 73. Although these apps appear to function normally to the user, when opened, they silently contact an Enterprise-operated C2 Server. Compl. ¶ 69; Decl. ¶ 73. The C2 Server then side-loads code on individual bots to request and render ads or instructs the device to download additional apps that request and render ads that are also hidden from the user. Compl. ¶ 69; Decl. ¶ 73. The Enterprise uses a "twin" strategy to disguise these malicious apps. Compl. ¶ 70; Decl. ¶ 74. The first "twin" is a "decoy twin," an app that does not contain malware and is available for download on legitimate app stores such as Google Play. Compl. ¶ 71; Decl. ¶ 75. The second app is the "evil twin." Compl. ¶ 72; Decl. ¶ 76. This app appears to be nearly identical to the decoy twin but is in fact malware that facilitates fraud. Compl. ¶ 72; Decl. ¶ 76. The close resemblance between the evil twin app and the decoy twin app prevents users from realizing that malware is present on their devices. Compl. ¶ 72; Decl. ¶ 76.

Certain members of the Enterprise operate as publishers of the apps or websites. Compl. ¶ 66; Decl. ¶¶ 67–68. They sell space for advertisements on the Enterprise's apps through publisher accounts on the Google Ad Network. Compl. ¶¶ 66–67; Decl. ¶ 67. Google pays publishers based on the number of times an ad is generated and viewed (i.e., impressions). Compl. ¶ 63; Decl. ¶ 64. Typically, Google only charges advertisers when a user takes an action after viewing the ad, such as clicking on the ad. Compl. ¶¶ 64–65; Decl. ¶¶ 65–66. Thus, when the Enterprise uses bots to generate or click on ads, the Enterprise-publisher receives payouts from Google. Compl. ¶ 66; Decl. ¶ 71. Google also refunds advertisers for fraudulent traffic, compounding its losses to the Enterprise's schemes. Compl. ¶ 67; Decl. ¶ 71.

Second, the BadBox 2.0 Enterprise also directs infected devices to interact with ads and submit fraudulent requests for ads on hidden web browsers that users cannot see. Compl. ¶¶ 78–80; Decl. ¶¶ 81–85. For example, the Enterprise publishes gaming websites and sells ad space on those domains through the Google Ad Network. Compl. ¶¶ 79–80; Decl. ¶¶ 82–85. The Enterprise uses the C2 Servers to command infected devices to navigate to the game websites and directs the bot to "play" the games. Compl. ¶¶ 79–80; Decl. ¶¶ 82–83. These games are designed to prompt an ad every few seconds, generating as many ad requests as possible, and triggering payouts from the Google Ad Network. Compl. ¶ 79; Decl. ¶ 84. The Enterprise also uses hidden web browsers to abuse paid search ad programs by directing bots to enter search strings and click on results, which generates search revenue for clicks on the Enterprise's websites without any real user ever clicking on the sponsored search result. Compl. ¶¶ 81–82; Decl. ¶¶ 86–87.

Third, the BadBox 2.0 Enterprise uses infected devices to carry out click fraud. Compl. ¶¶ 83–84; Decl. ¶¶ 88–89. The BadBox 2.0 Enterprise engages in click fraud when it uses C2 Servers to instruct bots to navigate to the Enterprise's low-quality web domains and click on advertisements hosted on those domains, resulting in a payout to the Enterprise. Compl. ¶¶ 83–84; Decl. ¶¶ 88–89. Here, too, Google also incurs costs when it refunds advertisers for the fraudulent traffic. Compl. ¶¶ 83–84; Decl. ¶¶ 88–89.

D. BadBox 2.0 Has Already Caused Significant Harm and Poses Still Greater Threats

The BadBox 2.0 botnet harms the owners of the infected devices, Google, and numerous other persons and entities. Compl. ¶ 86; Decl. ¶ 100. The owners of infected devices have had their devices and IP addresses hijacked and used to commit cybercrimes. Compl. ¶ 87; Decl. ¶ 96. They also may have had their personal information stolen. Compl. ¶ 87; Decl. ¶ 56. Indeed, Google has devoted (and continues to devote) substantial financial resources to investigate BadBox 2.0 and to identify measures necessary to remediate the harms caused by the botnet. Compl. ¶ 89; Decl. ¶ 101. Google also incurs losses from the Enterprise's ad fraud schemes; not only does it pay the Enterprise-publishers for ads generated on its fake platforms, but it also reimburses advertisers for fraudulent traffic. Compl. ¶¶ 61–67; Decl. ¶¶ 61–71. Google also experiences reputational damage and a loss of customer goodwill from the BadBox 2.0 Enterprise's actions. Compl. ¶¶ 90–92; Decl. ¶¶ 97, 102–104. Google's reputation is tarnished when ad fraud occurs on Google Ad Network. Compl. ¶ 91; Decl. ¶ 103.

The Enterprise's adaptation to efforts to disrupt its operation and its evolving tactics over time demonstrate that it is a sophisticated group with significant capabilities and reach. Compl. ¶ 4; Decl. ¶¶ 4–5, 90. Because it adds new bots—and therefore new computing power—daily, each day the Enterprise continues to operate unchecked, the threat it represents grows. Compl. ¶ 37; Decl. ¶¶ 4, 29. Google has identified activity related to BadBox 2.0 on its own platforms and has taken action to stop the impact of that activity. Decl. ¶¶ 31–32, 67–68. Until BadBox 2.0 is disrupted, the Enterprise will be able to continue conducting its criminal schemes, BadBox 2.0 will continue to grow in size and power, and the Enterprise will continue to generate revenue that it can reinvest in its schemes. Compl. ¶¶ 95–96; Decl. ¶¶ 94–96. With more than ten million devices already under its control, BadBox 2.0 can support large-scale cyber-attacks. Compl. ¶ 96; Decl. ¶ 98. The Enterprise could, for example, conduct or sell access to others to conduct large ransomware or DDoS attacks on legitimate businesses and other targets. Compl. ¶ 96; Decl. ¶ 98.

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 temporary restraining order 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 "decidedly" so, if the second factor is satisfied by sufficiently serious questions); and (4) "an injunction is in the public interest." *See 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). 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) (internal quotations omitted). Here, all of the injunction factors weigh 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 (internal quotations omitted). Courts have consistently granted preliminary relief in cases where, as here, the defendants are unknown persons or entities operating a botnet to harm the plaintiff and the public. *See, e.g.*, *Starovikov*, 2021 WL 6754263, at *1 (granting preliminary injunction against mix of known and unknown defendants for RICO, the Computer Fraud and Abuse Act ("CFAA"), and other statutory violations from botnet distribution of malware); *Microsoft*, 2016 WL 9334654, at *1 (granting preliminary injunction against two Doe defendants under the CFAA).[1]

[1] *See also, e.g.*, *Microsoft Corp. v. Does 1–51*, 2017 WL 10087886, at *1 (N.D. Ga. Nov. 17, 2017) (granting *ex parte* temporary restraining order against Doe defendants for CFAA violations from use of malicious computer code for botnet's illegal purposes); *Microsoft Corp. v. Does 1–8*, 2014 WL 12575722, at *1 (E.D. Va. June 27, 2014) (granting *ex parte* temporary restraining order against unknown defendants for CFAA violations stemming from use of botnet to send malicious computer code and injury plaintiff and its users); *Microsoft Corp. v. Does 1–82*, 2013 WL 2632612, at *1 (W.D.N.C. June 10, 2013) (ordering preliminary injunction on plaintiff's CFAA and RICO claims against unidentified defendants operating and commercializing a botnet with the purpose of stealing identification and personal security information and money, intruding upon plaintiff's software and its customers' devices, and intruding upon the protected devices of third parties, among other criminal actions).

This case is a quintessential candidate for emergency relief. The Enterprise is causing ongoing and irreparable harm to Google and the public. It is illegally infecting devices that run on modified-AOSP, selling proxy services through those devices, engaging in ad fraud that disrupts Google's business, causing Google (and numerous others) financial harm, impairing Google's reputation and goodwill, and defrauding unsuspecting consumers. Until the BadBox 2.0 botnet is disrupted, the Enterprise will continue to profit from its unlawful activities at the expense of Google and countless members of the public.

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

The BadBox 2.0 Scheme harms the owners of the infected devices, Google, and countless other persons and entities. Compl. ¶ 86; Decl. ¶ 99. The owners of infected devices are irreparably harmed: their devices and IP addresses have been commandeered to commit cybercrimes. Compl. ¶ 87; Decl. ¶ 100. Botnets can be programmed to steal personal information, financial information, usernames, and passwords from the owners of infected devices. Compl. ¶ 38; Decl. ¶ 29. They can also send emails without the owner of the infected device's knowledge or consent. Compl. ¶ 38; Decl. ¶ 29. These IP addresses may end up being identified as malicious, and then the user cannot use the device for normal activities. Compl. ¶ 55; Decl. ¶ 55. Owners and users of the infected devices cannot be made whole after this kind of personal invasion and identity theft. Compl. ¶ 87.

The BadBox 2.0 Scheme causes substantial and irreparable injury to Google as well. The BadBox 2.0 Enterprise's actions damage Google's goodwill and its reputation, which Google has cultivated over decades with the development of numerous products used by billions of people each day. Compl. ¶¶ 9, 90–92. Google's reputation is tarnished when ad fraud occurs on the Google Ad Network. Compl. ¶ 91; Decl. ¶ 103. Although Google does not own AOSP, because it originates from the Google-owned Android source code, Google retains a significant role in overseeing and approving development of AOSP to protect AOSP's and Google's reputation. Compl. ¶ 92; Decl. ¶ 102. 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 Church of Scientology*, 794 F.2d 38, 44 (2d Cir. 1986); *Microsoft Corp. v. Does 1–8*, 2015 WL 4937441, at *10 (E.D. Va. Aug. 17, 2015) ("[T]he surreptitious nature of the ... botnet is damaging to the Plaintiffs' brands and the customer goodwill engendered by their products and trademarks.").

In addition, Google has suffered and continues to suffer economic losses from the BadBox 2.0 Scheme. Google has utilized more than 25 employees and spent well in excess of $5,000 in a one-year period, investigating the BadBox 2.0 botnet, identifying necessary remediation, and seeking to protect Google and its users from the Enterprise's misconduct. Decl. ¶¶ 31, 101. Google also incurs losses from the Enterprise's ad fraud schemes—not only does it pay the Enterprise-publishers for ads generated on fake platforms, it also reimburses advertisers for fraudulent traffic. Compl. ¶¶ 61–67; Decl. ¶¶ 61–71. These expenditures are concrete and ongoing injuries to Google's business.

The irreparable harm to Google is especially clear given the high likelihood that it will never be made whole—even after final judgment—because the members of the Enterprise are unidentified and elusive cybercriminals who will take steps to avoid complying with any judgment. Decl. ¶ 90. "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." *Drobbin v. Nicolet Instrument Corp.*, 631 F. Supp. 860, 912 (S.D.N.Y. 1986).

B. Google Is Likely to Succeed on the Merits.

To obtain the relief sought, 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 trial." *Citigroup*, 598 F.3d at 34–35 (internal quotations omitted). Google not only raises serious questions going to the merits, but it is likely to succeed on each claim. Google has supported its motion with a declaration [redacted] detailing the substantial evidence of Defendants' misconduct. 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 CFAA Claims.

Congress enacted the CFAA to combat computer-related crimes, particularly "hacking or trespassing into computer systems or data." *United States v. Valle*, 807 F.3d 508, 525 (2d Cir. 2015) (internal quotations omitted). Courts routinely grant injunctive relief under the CFAA. *See, e.g.*, *Starovikov*, 2021 WL 6754263, at *3. The Enterprise has committed and is continuing to commit at least two independent violations of the CFAA. *First*, the Enterprise intentionally accesses protected computers without authorization, in furtherance of the intended fraud, to obtain value. 18 U.S.C. § 1030(a)(4). *Second*, the Enterprise knowingly causes the transmission of programs, information, codes, and/or commands to protected computers, intentionally causing damage. 18 U.S.C. § 1030(a)(5)(A). The Enterprise's violations of each of these provisions have caused loss to Google aggregating at least $5,000 in value during a one-year period, giving rise to this private action. *See* 18 U.S.C. § 1030(g); *id.* § 1030(c)(4)(A)(i)(I). Google has clearly established each of these elements.

First, Google's evidence establishes that the Enterprise accessed protected computers without authorization. *Id.* § 1030(a)(4). The Enterprise *accessed* the computers when it used malware to gain entry to data, software, and files on the computers. Compl. ¶ 101; *see Van Buren* *v. United States*, 593 U.S. 374, 388 & n.6 (2021) (defining "access"). The computers in this case are "*protected computers*" because they are used in communication through the internet. 18 U.S.C. § 1030(e)(2)(B); Compl. ¶ 100; Decl. ¶¶ 4, 24; *see Van Buren*, 593 U.S. at 379 (explaining that "all computers that connect to the Internet" are protected computers). Google's evidence shows that, as of April 2025, the Enterprise has accessed more than ten million computers. Compl. ¶ 39; Decl. ¶ 4. Finally, the Enterprise accessed those computers *without authorization*: the device owners did not consent to having the Enterprise infiltrate their devices or sell access to their computers to others. Decl. ¶ 55; *see Van Buren*, 593 U.S. at 389–90; 18 U.S.C. § 1030(e)(6).

Google has also shown that the Enterprise accesses these devices knowingly and with intent to defraud, its conduct furthers the intended fraud, and it obtains value. The Enterprise deliberately designs and distributes its malware to obtain access to infected computers with the intent to use them to conduct various criminal and fraudulent schemes, including ad fraud and selling proxy connections to infected computers (that in turn facilitate other cybercrimes), and it has succeeded in carrying out those fraudulent schemes. Compl. ¶¶ 41–85; Decl. ¶¶ 37–98. The Enterprise's conduct provides it value; it generates revenue from ad fraud and sales of proxy services to other cybercriminals. Compl. ¶ 51; Decl. ¶ 50.

Second, Google's evidence shows that the Enterprise also knowingly caused and is causing the transmission of programs, information, code, and/or commands and is intentionally causing damage to these protected computers. 18 U.S.C. § 1030(a)(5)(A). The Enterprise has intentionally transmitted software and commands to the infected devices through the BadBox 2.0 malware that has caused damage because the malware connects to the C2 Servers, and the C2 Servers download additional malware and send commands to engage with apps or web domains to generate or click on ads. Compl. ¶¶ 108–13; Decl. ¶ 42–48,73–89. "Damage" means "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). The Enterprise's transmission and use of the BadBox 2.0 malware damages infected devices by impairing their function and compromising their security. *See Van Buren*, 593 U.S. at 392 (explaining that "damage" refers to "technological harm[]—such as the corruption of files"); *United States v. Yücel*, 97 F. Supp. 3d 413, 419–21 (S.D.N.Y. 2015) (holding that malware that enables unauthorized remote access, causing a computer to "no longer operate[] only in response to the commands of the owner," damages that computer within the meaning of the CFAA).

Finally, regarding both CFAA provisions, Google has shown the damage affected well over ten computers within a one-year span and resulted in losses exceeding $5,000 within that timeframe, including the costs Google incurred in responding to and investigating the botnet's harmful proliferation, including conducting damage assessments. Decl. ¶¶ 101–103; *see* 18 U.S.C. § 1030(g); *id.* § 1030(c)(4)(A)(i)(I), (VI); s*ee also Saunders Ventures, Inc. v. Salem*, 797 F. App'x 568, 572–73 (2d Cir. 2019) (holding that costs of an investigation "to identify evidence of a breach, to assess any damage it may have caused, and to determine whether any remedial measures were needed" qualify as compensable "loss" under the CFAA); *Univ. Sports Publ'ns Co. v. Playmakers Media Co.*, 725 F. Supp. 2d 378, 387–88 (S.D.N.Y. 2010).

The BadBox 2.0 Enterprise's infiltration of infected computers and theft of information is precisely the activity the CFAA is designed to prevent. As the Second Circuit has observed, the Act was "enacted . . . to address 'computer crime,'" which was "principally understood as 'hacking' or trespassing into computer systems or data." *Valle*, 807 F.3d at 525 (quoting H.R. Rep. No. 98-894, at 6–10); *see also Microsoft Corp. v. Does 1–18*, 2014 WL 1338677, at *6 (E.D. Va. Apr. 2, 2014) ("The CFAA was designed to prevent the sort of unauthorized access and other fraudulent activity effectuated by malware and botnet activity"). Accordingly, courts have consistently upheld relief under the CFAA in circumstances similar to those presented here. *See, e.g.*, *Microsoft Corp. v. Does 1–2,* 2021 WL 4260665, at *3 (E.D.N.Y. Sept. 20, 2021) (granting default judgment to Microsoft where defendants allegedly used a botnet to infect Microsoft customers' computers and access their data); *Starovikov*, 2021 WL 6754263, at *1 (granting preliminary injunction where defendants allegedly used a botnet to intentionally infect thousands of computers with malware to steal information); *Microsoft Corp. v. Does 1–51*, 2018 WL 3471083, at *1 (N.D. Ga. June 18, 2018) (granting TRO where defendants allegedly used a botnet to infect Microsoft customers' computers and steal sensitive information); *Facebook, Inc. v. Fisher*, 2009 WL 5095269, at *1 (N.D. Cal. Dec. 21, 2009) (granting TRO where defendants allegedly engaged in a spamming and phishing scheme designed to steal Facebook login credentials); *Physicians Interactive v. Lathian Sys., Inc.*, 2003 WL 23018270, at *6 (E.D. Va. Dec. 5, 2003) (granting TRO where defendant allegedly used software to hack a website and file server to obtain proprietary information without authorization); Declaration of Laura Harris, dated May 27, 2025, ¶ 11, n.1 (collecting cases).

For all of these reasons, Google's CFAA claim is likely to succeed on the merits.

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

Google is likely to prevail on its claims under RICO. 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). It 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). 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 (2d Cir. 2024).

The BadBox 2.0 Enterprise is the modern incarnation of organized crime, and its fraudulent activities have occurred not only in New York, but across the country and beyond. Google can satisfy each of the required elements of a RICO claim for each Defendant. As set out above, it has suffered injury to its business or property as a result of the Enterprise's racketeering activity.

1. **Conduct.** To establish the conduct element, a plaintiff must establish that the defendant 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.* (internal quotations omitted). Here, each Defendant had at least "some part" in the BadBox 2.0 Enterprise. *Id.*; *see* Compl. ¶¶ 41–45; Decl. ¶¶ 37–40. Members of the Enterprise all take part in directing the aspects of the scheme: some develop the botnet infrastructure; others sell proxy access to IP addresses to mask and facilitate nefarious internet activity; others render hidden ads on apps and preinstalled on infected devices; still others launch hidden web browsers that load hidden ads; and yet others steer infected devices to domains managed by the Enterprise, all to enrich themselves. *See* Compl. ¶¶ 41–45; Decl. ¶¶ 37–40. The Enterprise works together to implement their schemes; none of the schemes can generate revenue without the Enterprise members' cooperation. *See* Compl. ¶ 45; Decl. ¶¶ 37–40.

2. **Enterprise.** To show that 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)). To "participate in" the conduct of an enterprise's affairs, "one must have some part in directing those affairs." *Reves v. Ernst & Young*, 507 U.S. 170, 179 (1993) (internal quotations omitted). This is a low bar, "especially at the pleading stage." *1st Cap. Asset Mgmt., Inc. v.*

Satinwood, Inc., 385 F.3d 159, 175–76 (2d Cir. 2004). The Enterprise members' common purpose is clear: deploy malware to infect smart devices to build a botnet, sell proxy access to that botnet for numerous criminal schemes, and use the botnet to engage in a variety of ad fraud schemes to further enrich the Enterprise. Compl. ¶ 46; Decl. ¶ 4. The Enterprise is organized to carry out these aims together and function as a unit, as evidenced by its use of a shared infrastructure (the C2 Servers and domains) and its historical and continuing business ties. Compl. ¶ 44; Decl. ¶ 40. There are numerous connections between the members of the Enterprise and the domains through which they conduct the BadBox 2.0 Scheme; indeed, many of them were involved in the original BadBox botnet. Compl. ¶¶ 30, 42, 44; Decl. ¶¶ 37–40. Google has therefore provided strong evidence to show that the members of the Enterprise 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 continuity 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)). Google has presented numerous examples of the Enterprise's recent criminal conduct that clearly forms a "pattern" within the meaning of the statute. Compl. ¶¶ 46–85; Decl. ¶¶ 49–89. That pattern is continuous because there is undoubtedly a threat, if not a virtual certainty, of continuing criminal activity; indeed, the fraudulent schemes are still operating today and show no signs of slowing. *Spool v. World Child Int'l Adoption Agency*, 520 F.3d 178, 183 (2d Cir. 2008); *see also United States v. Aulicino*, 44 F.3d 1102, 1111 (2d Cir. 1995) (finding that continuity can also be demonstrated where, as here, the aims of the enterprise are inherently unlawful). The BadBox 2.0 Enterprise aims to perpetuate the sale of proxy connections for criminal purposes and to perpetuate its unlawful ad fraud schemes.

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 CFAA, 18 U.S.C. § 1030, and the federal wire fraud statute, 18 U.S.C. § 1343. As detailed in the Complaint, Defendants violated the CFAA in multiple ways, including by infecting users' computers with malware to infiltrate their systems and give the C2 Servers persistent access to the device. Compl. ¶ 50, Decl. ¶ 47. The C2 Servers can instruct the device to install additional malware modules to support the Enterprise's criminal activity and send commands to the infected devices. Compl. ¶ 50; Decl. ¶ 48. The Enterprise's violations of the CFAA have damaged more than ten protected computers during a one-year period—in fact, they have damaged millions of protected computers. Decl. ¶¶ 4, 30; *see* 18 U.S.C. § 1030(c)(4)(A)(i)(VI).

The BadBox 2.0 Enterprise also committed wire fraud in at least two ways 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. *First*, the Enterprise defrauds users each time it tricks them into downloading an app loaded with BadBox 2.0 malware by mimicking non-malware apps. *Second*, each time that the Enterprise uses a bot to mimic a real user and sends a bid request to the Google Ad Network, the Enterprise deceives Google as to the true nature of the bid request.

Finally, 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 connections among the Enterprise members indicate that the Enterprise formed an agreement to undertake the acts described above as part of a common scheme and conspiracy. Compl. ¶¶ 41–45; Decl. ¶¶ 37–

41. Because they agreed to form and operate the BadBox 2.0 botnet and to commit the numerous predicate acts of fraud and related activity that make up the criminal activity facilitated by the botnet, Defendants are liable under 18 U.S.C. § 1962(c).

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

The equities also favor a temporary restraining order. The BadBox 2.0 Enterprise damages consumers' devices, commits fraud, enables other cybercriminals to commit crimes, and injures Google. There is no conceivable reason why the Enterprise should be permitted to continue to weaponize harmful malware at the expense of Google and the public. *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 temporary restraining order where the Enterprise's practices likely violate a federal statute). Further, in a CFAA case such as this one, where the requested relief is to restrain plainly illegal and harmful behavior, the balance of equities favors such relief. *Microsoft Corp. v. Does 1–2*, 2021 WL 8444748, at *7 (E.D. Va. Aug. 12, 2021) ("The balance of equities tips in favor of granting an injunction when the enjoined activity involves an illegal scheme to defraud computer users and injure Plaintiffs"), *report and recommendation adopted*, 2021 WL 8444640 (E.D. Va. Sept. 24, 2021).[2]

[2] *See also Microsoft Corp. v. Does 1–2*, 2024 WL 1708328, at *11 (E.D. Va. Jan. 10, 2024) ("Defendants would not suffer any hardship because an injunction would only require them to cease engaging in illegal activities"), *report and recommendation adopted*, 2024 WL 1708323 (E.D. Va. Jan. 30, 2024); *Dow Corning Corp. v. Chaganti*, 2015 WL 6735335, at *11 (E.D. Mich. Nov. 4, 2015) (ruling that "it is hard to conceive of a party that would be truly harmed by the imposition of a restraining order" in CFAA case involving unlawful access to protected information and devices).

D. The Public Interest Favors a Temporary Restraining Order.

Finally, a temporary restraining order would serve the public interest. First, the public interest is clearly served by enforcing statutes designed to protect the public, such as the CFAA and RICO. *See, e.g.*, *Fla. Atl. Univ. Bd. of Trs. v. Parsont*, 465 F. Supp. 3d 1279, 1298 (S.D. Fla. 2020). Second, it is in the public's interest to permit Google to take the necessary steps to eliminate BadBox 2.0. The BadBox 2.0 botnet has infiltrated over ten million consumer devices. Compl. ¶¶ 1, 39; Decl. ¶ 4. With each day that passes, the Enterprise infects and damages more devices, defrauds more victims, and facilitates more crimes by other cybercriminals. Compl. ¶¶ 1, 93–96; Decl. ¶¶ 4, 94–96. The longer the botnet is allowed to grow, the more threatening it becomes, and the greater the risk it will pose, as it can be deployed to commit DDoS attacks and spread ransomware or propaganda, including to interfere with elections or influence public policy.[3] Compl. ¶ 96; Decl. ¶¶ 94–98.

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

Rule 65 authorizes courts to enter a temporary restraining order *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 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

[3] Ctr. for Internet Sec., *Election Security Spotlight – Bots* (2025), https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-bots; Christopher Bing, *Exclusive: U.S. officials fear ransomware attack against 2020 election*, Reuters (Aug. 27, 2019), https://www.reuters.com/article/us-usa-cyber-election-exclusive/exclusive-u-s-officials-fear-ransomware-attack-against-2020-election-idUSKCN1VG222/; Tom Burt, *New action to combat ransomware ahead of U.S. elections*, Microsoft (Oct. 12, 2020), https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/.

why it should not be required." *Id.* A temporary restraining order "may be ordered on an ex parte basis under subdivision (b) if the applicant makes a strong showing of the reasons why notice is likely to defeat effective relief." Fed. R. Civ. P. 65 committee notes to 2001 amendment. As such, even where 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 Fils S.A.*, 606 F.2d 1, 5 (2d Cir. 1979) (per curiam); *see also Granny Goose Foods, Inc. v. Bhd. of Teamsters & Auto Truck Drivers Loc. No. 70*, 415 U.S. 423, 439 (1974).

Google has already set forth facts demonstrating immediate and irreparable harm. Advance notice should not be required here because if the Enterprise were notified of the relief Google is seeking before this Court issues a temporary restraining order, it would quickly transfer or otherwise dissipate the infrastructure and resources supporting the BadBox 2.0 Scheme, *see* Decl. ¶ 90, which would prevent Google from disrupting the infrastructure. Because notice would render relief ineffective, an *ex parte* temporary restraining order is appropriate. *See In re Vuitton*, 606 F.2d at 5.

The BadBox 2.0 botnet is sophisticated, and the Enterprise can quickly reshuffle its infrastructure to ensure its survival. *See* Decl. ¶ 90. Indeed, the Enterprise created its present operation in the wake of the disruption of the original BadBox botnet. *See* Compl. ¶ 4; Decl. ¶ 5. The effectiveness of Google's requested relief therefore depends largely on it being implemented before the Enterprise knows about it. Decl. ¶ 90. Courts in this district and throughout the country have consistently found that defendants engaged in illicit internet enterprises, including the use of botnets, are "likely to delete or to relocate" the harmful code, "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." *Sophos Ltd. v. Does 1–2*, 2020 WL 4722425, at *2

(E.D. Va. May 1, 2020); *see also, e.g.*, *Ex Parte* Temporary Restraining Order at 14, *Google LLC v. Starovikov*, No. 1:21-cv-10260-DLC (S.D.N.Y. Dec. 7, 2021), ECF No. 8; *Ex Parte* Temporary Restraining Order and Order to Show Cause at 3, *FTC v. Pricewert LLC*, No. 5:09-cv-2407-RMW (N.D. Cal. June 2, 2009), ECF No. 12 (issuing *ex parte* temporary restraining order suspending internet connectivity of a company enabling botnet activity because otherwise the "[d]efendant is likely to relocate the harmful and malicious code").

This case presents the same danger. The Enterprise's technological sophistication and ability to move its domains and servers quickly pose a significant risk, if not certainty, that the BadBox 2.0 Scheme will continue if the Enterprise is given advance notice of Google's requested relief. Decl. ¶ 90. To ensure that the *ex parte* relief is strictly limited to "serving [its] underlying purpose" and no more, *Granny Goose Foods*, 415 U.S. at 439, if the proposed order is granted, then Google will undertake extraordinary efforts to provide actual notice to the Enterprise of the temporary restraining order and preliminary injunction hearing, and effect service of the Complaint, order, and other papers filed in this matter, immediately upon effectuation of the injunctive relief in the proposed order, and in no event fewer than five days before the preliminary injunction hearing (or such time as the Court may order).

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

Google also requests permission to serve the Enterprise's members, who are believed to reside in China, by alternative means under Federal Rule of Civil Procedure 4(f)(3). Compl. ¶ 10; Decl. ¶ 4. Google requests authorization to serve the Enterprise through as many of the following methods as are available: (1) mail; (2) email using any information available from web-hosting companies provided in connection with domain names used in the BadBox 2.0 botnet and/or any email addresses identified through Google's investigation; and (3) website publication.

Courts may authorize service through a variety of methods, "including publication, ordinary mail, mail to the defendant's last known address, delivery to the defendant's attorney, telex, and most recently, email." *Rio Props., Inc. v. Rio Int'l Interlink*, 284 F.3d 1007, 1016 (9th Cir. 2002). To satisfy due process requirements, notice must be "reasonably calculated, under all the circumstances, to apprise interested parties of the pendency of the action and afford them an opportunity to present their objections." *Chase Grp. All. LLC v. City of N.Y. Dep't of Fin.*, 620 F.3d 146, 150 (2d Cir. 2010) (quoting *Mullane v. Cent. Hanover Bank & Tr. Co.*, 339 U.S. 306, 314 (1950)). All that is required is "the best notice practical under the circumstances." *In re Drexel Burnham Lambert Grp. Inc.*, 995 F.2d 1138, 1144 (2d Cir. 1993). Here, emails—if available—are likely to be the most accurate and viable means of notice and service for this cybercriminal Enterprise. Other courts have authorized service by email in similar circumstances. *See, e.g.*, *Microsoft*, 2014 WL 1338677, at *3; *Rio Props.*, 284 F.3d at 1014–18. In addition, "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).

As further confirmation that Google's proposed methods of service are reasonably calculated to provide actual notice and appropriate in these circumstances, Google will send notice by ordinary mail to the extent an address is available. The Court should therefore authorize Google's request for alternative service in accordance with the accompanying proposed order.

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

The Enterprise uses apps, domains, and web servers hosted by third parties to perpetuate its fraud against Google and the public. Google's proposed order, if entered by the Court, would direct these third-party registrars, web infrastructure companies, and web hosting providers to take down, suspend, or sinkhole the infrastructure used by the Enterprise, thereby disrupting its schemes. Decl. ¶¶ 91–93. This relief would include the disruption of any IP addresses or domains that the Enterprise may use in the future to perpetrate the BadBox 2.0 botnet that are currently unknown to Google or that do not currently exist. 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. Under well-established precedent, this language empowers courts to issue orders to non-parties. The power conferred by the Act extends, 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, such 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), *report and recommendation 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. Ca. Nov. 7, 2023). The same is true for the hosting companies that maintain the servers. *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 and servers that enable the Enterprise to perpetrate its crimes.

In keeping with these principles, district courts across the country have invoked the All Writs Act to grant relief similar to the relief requested here. *See, e.g.*, *Microsoft Corp. v. Does 1–82*, 2013 WL 6119242, at *3 (W.D.N.C. Nov. 21, 2013) (noting that the defendants had "engaged in illegal activity using the Internet domains" and ordering that the specified domains be "immediately transferred to the ownership and control of Microsoft").[4] To protect the public from

[4] *See also Microsoft*, 2014 WL 1338677, at *12–13 (ordering registrars of domains associated with a botnet to "transfer the domains ... to the control of Microsoft"); *Microsoft*, 2017 WL 10087886, at *4 (ordering registrars to "tak[e] … reasonable steps to work with Microsoft to ensure the redirection of the domains and to ensure that Defendants cannot use them to control the botnets"); *Microsoft*, 2021 WL 4260665, at *4 (ordering domain registrars to "take reasonable steps to ... prevent the domains from being controlled by the Defendants"); *Starovikov*, 2021 WL 6754263, at *1.

the serious threat posed by the BadBox 2.0 botnet, it is well within this Court's authority to order the takedown or transfer of the domains and servers specified in **Appendix A** to the Complaint and to authorize Google to seek additional intervention from the Court in the event that Google identifies additional entities associated with or domains used in connection with BadBox 2.0.

CONCLUSION

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

Dated: May 27, 2025

Respectfully submitted,

Laura Harris
KING & SPALDING LLP
1185 Avenue of the Americas, 34th Fl.
New York, NY 10036-2601
Tel: (212) 556-2100
Fax: (212) 556-2222
lharris@kslaw.com

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

Counsel for Plaintiff Google LLC

CERTIFICATE OF COMPLIANCE

I, Laura Harris, an attorney duly admitted to practice before this Court, hereby certify pursuant to Local Rule 7.1(c), that the foregoing Google LLC's Memorandum of Law in Support of Its Motion for an *Ex Parte* Temporary Restraining Order and Order to Show Cause was prepared using Microsoft Word and contains 8,736 words in accordance with Local Rule 7.1(c).

Dated: May 27, 2025

Laura Harris