

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC,

Plaintiff,

v.

DMITRY STAROVIKOV;
ALEXANDER FILIPPOV;
and Does 1-15,

Defendants.

Civil Action No.

FILED UNDER SEAL

COMPLAINT FOR DAMAGES AND INJUNCTIVE RELIEF

Plaintiff Google LLC (“Google”) for its Complaint against the Defendants listed below alleges as follows:

INTRODUCTION

1. Defendants are Russian cybercriminals who have silently infiltrated more than a million computers and other devices around the globe to create a network—the Glupteba “botnet”—to use for illicit purposes, including the theft and unauthorized use of Google users’ login and account information. Defendants use the Glupteba botnet to further a range of cybercrimes and to conceal criminal conduct. And at any moment, the power of the Glupteba botnet could be leveraged for use in a powerful ransomware¹ or distributed denial-of-service (“DDoS”) attack.²

2. The Glupteba botnet is distinguished from conventional botnets in its technical sophistication: unlike other botnets, the Glupteba botnet leverages blockchain technology to protect itself from disruption.

3. Defendants Dmitry Starovikov, Alexander Filippov, and other unknown individuals work in concert to grow, control, and profit from the Glupteba botnet. Defendants and their criminal enterprise (hereinafter referred to as the “Glupteba Enterprise” or the “Enterprise”) represent a modern technological and borderless incarnation of organized crime. The Glupteba Enterprise operates through a network

¹ Ransomware is an increasingly common type of malicious software (“malware”) that is designed to block access to all or part of a computer system until a sum of money is paid.

² A DDoS attack occurs when multiple internet-connected devices are directed to collectively overwhelm the bandwidth of a particular website or system for the purpose of taking that website or system offline.

of individuals and organizations that, together, engage in and profit from a pattern of criminal racketeering conduct.

4. The Glupteba Enterprise uses its illicit access to devices infected with Glupteba malware to further numerous criminal schemes, including:

- a. **Stolen Accounts Scheme:** Stealing personal account information (including Google and other account login information) from infected devices and selling to third parties access and use of the stolen accounts through virtual machines preloaded with those accounts;
- b. **Credit Card Fraud Scheme:** Selling credit cards for fraudulent purchases from Google. These credit cards pass technical authorization checks but have insufficient funds to pay for the services or goods purchased for use in connection with the Stolen Accounts Scheme, resulting in the purchase of ads or services from Google (and other web-based companies) for which payment is not made;
- c. **Disruptive Ad Scheme:** Selling the placement of disruptive ads (*e.g.*, pop-up ads in videos) on infected devices whose victim owners are unwitting to the scheme;
- d. **Proxy Scheme:** Selling unauthorized access to victims' infected devices for use as "residential proxies," which, unbeknownst to the victims, are exploited by cybercriminals to conceal their location and internet protocol ("IP") address while committing other crimes;

e. **Cryptojacking Scheme:** Hijacking (or “cryptojacking”) the computing power of infected devices to generate cryptocurrency for the Glupteba Enterprise’s financial gain.

5. The Glupteba Enterprise is responsible for causing significant harm to Google, Google users, the owners of infected devices, and countless other entities and individuals.

6. The Glupteba Enterprise causes financial harm to Google, interferes with Google’s relationships with its users (and potential users), harms Google’s reputation, impairs the value of Google’s trademarks, and forces Google to devote substantial resources to combat the Enterprise’s harmful activity.

7. Google brings this action under the Racketeer Influenced and Corrupt Organizations Act (“RICO”), Computer Fraud and Abuse Act, Electronic Communications Privacy Act, Lanham Act, and New York law, against Defendants’ criminal enterprise to disrupt the Glupteba botnet, to prevent it from causing further harm, and to recover damages.

PARTIES

Plaintiff

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

9. 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 largest, most effective,

and 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.

10. Google operates numerous products, platforms, and services, several of which are core to its business and relevant here:

- a. **Android:** Android is an operating system that is designed to run on mobile devices, such as smartphones or tablets.
- b. **Chrome:** Chrome is a web browser that runs on various operating systems, including on personal computers, smartphones, and tablets.
- c. **Gmail:** Gmail is an email service that is hosted on Google's servers.
- d. **Google Drive:** Google Drive is a file storage service that allows users to host and share files in various formats on Google's servers. These files can be created, accessed, and edited remotely.
- e. **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.
- f. **Google Workspace:** Google Workspace is a cloud-based suite of productivity and collaboration tools for businesses. This service

provides businesses with custom email accounts with integrated collaboration tools, including Gmail, Google Calendar, Google Meet, Google Chat, Google Drive, Google Docs, Google Sheets, Google Slides, Google Forms, and Google Sites.

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

11. 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 malware such as the Glupteba botnet.

12. Google supports its businesses in part through revenue generated by its many advertising products, all geared toward delivering relevant ads and providing consumers with useful commercial information. Google's broad suite of advertising and analytics tools help millions of companies grow their businesses every day.

13. Google constantly invests in and improves its advertising programs. Today, Google Ads is a world-class ad technology platform for advertisers, agencies, and publishers to power their digital marketing or monetization. A core focus of the product is serving relevant ads at the right time in a non-intrusive manner, and ensuring advertisers have effective tools to target and measure the effectiveness of their ad campaigns.

14. Google has allocated, and continues to allocate, substantial resources to restricting fraudulent ads and protecting users on the web. These include, among other things, filtering out invalid traffic, removing bad actors and billions of improper ads from Google systems every year, and closely monitoring the sites, apps, and videos where ads appear to ensure that ads do not fund bad content.³

Defendants

15. The defendants listed in paragraphs 16 and 17 are individuals who have conspired to engage in a pattern of racketeering activity. They each have participated in the operation or management of the Glupteba Enterprise and have engaged in criminal acts causing harm to Google and countless others.

16. Defendant Dmitry Starovikov is an individual who resides in Russia.

17. Defendant Alexander Filippov is an individual who resides in Russia.

18. Plaintiff does not know the true names and capacities of the Doe Defendants sued as Does 1 through 15, and therefore sues these defendants by such fictitious names. Each of the Doe defendants is responsible in some manner for the conduct alleged, having agreed to become part of the Glupteba Enterprise.

³ In 2020, Google disabled 1.7 million advertiser accounts and removed roughly 3.1 billion ads for violating its policies, including 867 million ads that abused the ad network by attempting to evade Google's detection systems and lure users off Google's platforms with an aim to defraud them. Scott Spencer, Our Annual Ads Safety Report, Google Ads & Commerce Blog (Mar. 17, 2021), <https://blog.google/products/ads-commerce/ads-safety-report-2020>.

JURISDICTION AND VENUE

19. This Court has federal-question jurisdiction over Google's claims under RICO, the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act, and the Lanham Act under 28 U.S.C. § 1331. This Court also has jurisdiction over the Lanham Act and related state and common law unfair competition claims under 28 U.S.C. § 1338, and 15 U.S.C. § 1121. This Court has supplemental jurisdiction over the state-law claims under 28 U.S.C. § 1367.

20. Defendants are subject to personal jurisdiction in this district, and the exercise of jurisdiction over Defendants is proper pursuant to 18 U.S.C. § 1965 and N.Y. C.P.L.R. §§ 301 and 302. Defendants have transacted business and engaged in tortious conduct in the United States and in New York which gives rise in part to Google's claims. Defendants also have engaged in intentional, wrongful, illegal, and/or tortious acts, the effects of which Defendants knew and intended would be felt in the United States and New York. Among other things, Defendants have intentionally caused Glupteba malware to be downloaded on victims' machines in this district, in New York, and throughout the United States; have intentionally directed victims' machines in this district, in New York, and throughout the United States to participate in intentional, wrongful, illegal, and/or tortious acts; and have directed multiple forms of communication to co-conspirators in 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.

21. 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 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 availing themselves of the privilege of conducting business in New York, and utilize instrumentalities located in this judicial district to carry out acts alleged herein.

22. Defendants have affirmatively directed actions at New York and the Southern District of New York by directing their activities, including theft of funds, hardware, and information, at individual computer users located in the Southern District of New York. Defendants have directed malicious computer code at the computers of individual users located in New York and the Southern District of New York. Defendants have attempted to and, in fact, have infected such user computers with malicious computer code.

FACTUAL ALLEGATIONS

Botnets

23. Most botnets spread through a simple malware download. “Malware” is “malicious software” that is generally designed to damage, destroy, disrupt, or steal data from a computer system.

24. Most users of a computer or other device install malware inadvertently. For example, the user is encouraged to click on a link, interact with an online advertisement, or open an attachment to an email, and unknowingly triggers the download and installation of the malware on the user’s device. In colloquial terms, the device is then infected with a computer virus.

25. A “bot” (short for “robot”) is a computer or device that is infected by malware and that can be tasked to conduct specific activities.

26. A “botnet” is a network of internet-connected devices (bots), each of which are infected by malware. The botnet is controlled by “command-and-control” (“C2”) servers, which can instruct the devices comprising the botnet to perform any number of disruptive or even criminal tasks. The C2 servers typically are controlled remotely by individual operators, referred to as “bot controllers.”

27. The botnet’s computing power grows with each new device that is infected. Thus, depending on the volume of devices comprising the botnet, the bot controllers can marshal an astonishing amount of computing power to commit cybercrimes. For example, botnets can be used to orchestrate DDoS attacks, in which numerous computers (without the owners’ knowledge) simultaneously send requests

to a single website or resource. The attack can overwhelm the target, rendering the website or other internet-based service unusable.

28. Botnets also can be programmed to steal personal information, financial information, usernames, and passwords from infected devices. They can send emails without the owner of the infected device's knowledge or consent. They can "proxy" or "relay" internet communications to mask the location of bad actors, thereby concealing and facilitating criminal conduct. They can send additional malware to infect other computers. And they can act as a vector to spread ransomware or propaganda, including to interfere with elections or influence public policy. In other words, botnets are both powerful and flexible tools to commit cybercrimes.

The Glupteba Botnet

29. Cybersecurity experts first noticed Glupteba malware in 2011, when it was primarily associated with a spam campaign. In recent years, however, the spread of Glupteba malware has increased substantially and the botnet has become markedly more dangerous. Google estimates that it has infected more than one million computers and other devices.

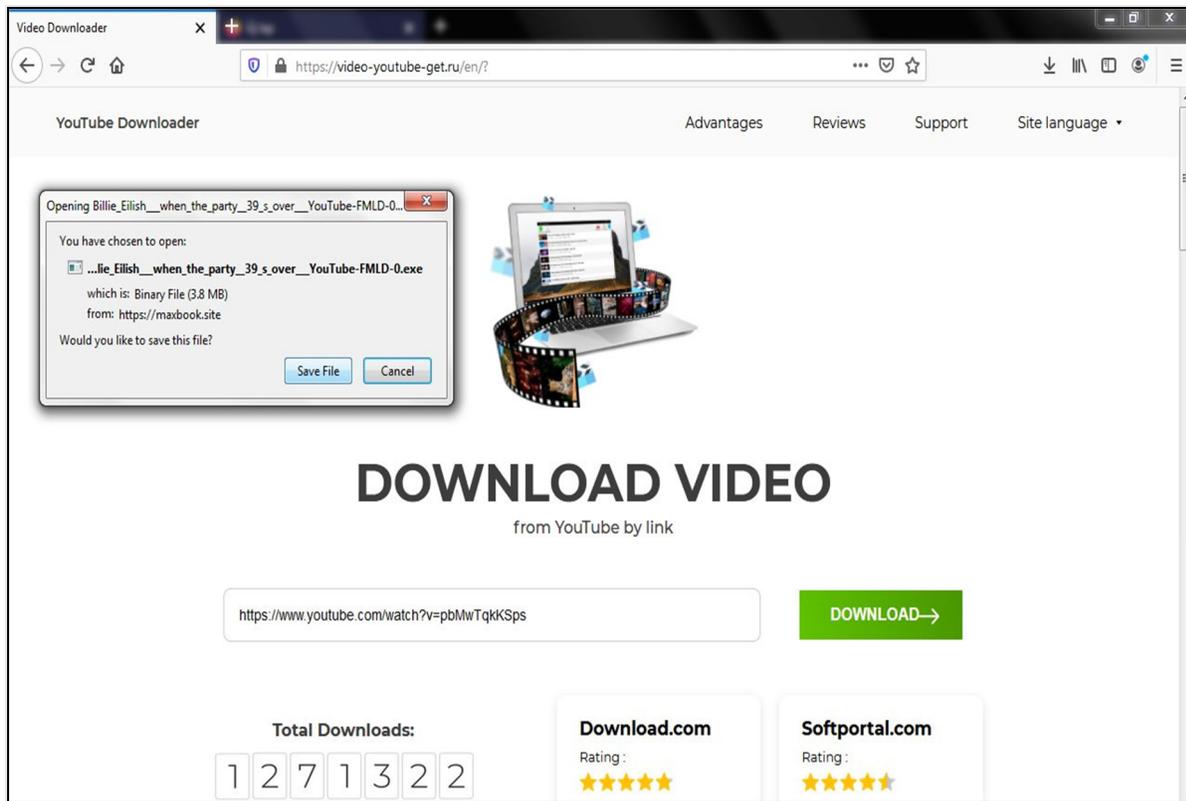
30. In the summer of 2020, Google determined that Glupteba malware was being disseminated on numerous third-party software download sites, online movie streaming sites, and video downloader sites, often advertised as "free downloads."

31. Glupteba malware masquerades as free, downloadable software, videos, or movies ("freeware") and infects a device when a user clicks on a link to the

freeware. For example, users who click on a link looking to download a free game instead unknowingly download and install Glupteba malware.

32. The Glupteba Enterprise and its agents distribute these links through pay-per-install arrangements by which the Enterprise pays its agents for each successful installation of the malware. The Enterprise and its agents abuse well-established and famous trademarks in order to capture consumers' attention and trick them into believing that the trademarks represent trusted brands. These abuse campaigns are frequently short-lived and quickly change from one entity to another, so that the Enterprise stays ahead of trademark owners' ongoing efforts to stop infringement and abuse.

33. For example, as reflected in the image below, the Glupteba Enterprise unlawfully leveraged a well-known Google mark—YouTube—to help disseminate Glupteba malware. At the website located at “video-youtube-get.ru,” users were deceived, in part due to the use of “youtube” in the domain name and on the landing page, into believing they were downloading a YouTube video. When users clicked on the link to download the video, they unknowingly downloaded and installed Glupteba malware on their devices.



34. When an unsuspecting victim clicks on one of Glupteba-hosting links, the malware is delivered to the victim’s device via “droppers.” Droppers are a type of Trojan horse virus: they appear as a legitimate application to the user, but once downloaded, they deliver malware to the user’s device.

35. Glupteba is a modular malware, meaning that it installs new modules with different functionality over time as instructed by the Glupteba Enterprise.

36. The Glupteba botnet uses various domain names⁴ that point to IP addresses that host two different types of servers—content delivery network (“CDN”) servers and C2 servers—to download and execute the modules. These domain names

⁴ The domain name is a “pointer” to an IP address where a server is hosted.

are hard-coded in the malware and can be refreshed through backdoor functions⁵ or by querying the blockchain, explained *infra* at paragraphs 41 to 50. **Appendix A** lists the known domains⁶ and IP addresses used by the Glupteba Enterprise, as well as the registrars⁷ for each domain.

37. Once the Glupteba malware's main dropper component is installed on a device, the botnet delivers additional modules to that device. Modules are then executed as instructed by the C2 server, which is operated by the Glupteba Enterprise.

38. The first executed module acts as a scout to detect the security system in place on the computer (or other device), so that the Glupteba malware can evade detection by the device's owner and antivirus software. It manipulates the owner's operating system by hiding the malware's existence and preventing it from revealing itself on an infected device's security logs. The module is designed to circumvent cybersecurity detection tools, anti-virus software, and system monitoring programs, including security software featured in popular operating systems.

39. The Glupteba Enterprise then uses various other modules to execute its criminal schemes, explained *infra* at paragraphs 51 to 88.

⁵ Backdoor functions are covert methods of bypassing normal authentication or encryption in an internet-connected device.

⁶ **Appendix A** includes domains used for C2 and CDN server communication and operation, as well as domains used for distribution of the Glupteba malware and domains used for the Enterprise's criminal schemes.

⁷ Registrars obtain domain rights for their customers from registry services that are responsible for managing domains.

40. Once the modules are downloaded to the infected device via the CDN server, the C2 server communicates commands to the infected device to control it and utilize those modules. For example, the C2 server could activate the “*steal credentials from this device*” module or the “*use this device for cryptocurrencies mining*” module, depending on the Glupteba Enterprise’s plans for the infected device.

The Glupteba Botnet Leverages Blockchain Technology

41. Unlike conventional botnets, the Glupteba botnet leverages the blockchain technology used in certain cryptocurrency transactions to protect critical lines of communication between the C2 servers and the botnet that they direct.

42. Cryptocurrency is a digitized data currency, rather than a physical currency like a coin or a dollar bill, that uses advanced cryptography to secure transactions. A particularly well-known form of cryptocurrency is called Bitcoin. Many cryptocurrencies, including Bitcoin, use blockchain technology as a public, distributed ledger to record cryptocurrency transactions. Each time a transaction occurs, a new entry or “block” of information is created. These blocks are then joined together in a “chain.”

43. Critically, no administrator has control of the cryptocurrency transaction information recorded in the blockchain. The transaction information is permanently recorded and, in many cases, viewable to anyone.

44. People own cryptocurrencies, such as Bitcoin, through digital “wallets,” which are software-based digital payment services or applications that interface with the blockchain. Wallets interface with a cryptocurrency’s blockchain and store the

public and private “keys” used to send and receive cryptocurrency. A public key, or “address,” is akin to a bank account number, and a private key is akin to a PIN or password that allows a user the ability to access and transfer value associated with the public address and the private key. To conduct transactions on a blockchain, an individual must use the public address and the corresponding private key.

45. The blockchain, which is run by the decentralized network for a particular cryptocurrency, contains the historical records of every transaction in that currency (the “blocks”). On the Bitcoin blockchain, the public addresses of those engaging in Bitcoin transactions are recorded, but the identities of the individuals or entities behind those public addresses are not.

46. A conventional botnet does not use blockchain to maintain lines of communication between C2 servers and infected devices. Rather, in a conventional botnet, infected devices are programmed to look for pre-determined domain addresses that point to the C2 server. The instructions to locate those domains are hard-coded in the malware. If the predetermined domains are shut down (by law enforcement or others), the infected devices can no longer receive instructions from the C2 servers and therefore can no longer be operated by the bot controller. For that reason, conventional botnet operators may utilize thousands of “disposable” domains (using domain generation algorithms) to defend against law enforcement action to disrupt the botnet.

47. Unlike conventional botnets, the Glupteba botnet does not rely solely on predetermined domains to ensure its survival. Instead, when the botnet’s C2 server

is interrupted, Glupteba malware is hard-coded to “search” the public Bitcoin blockchain for transactions involving three specific Bitcoin addresses that are controlled by the Glupteba Enterprise. From time to time, the Glupteba Enterprise executes transactions in those addresses, and as part of those transactions, the Glupteba Enterprise leaves in the blockchain the location of the domain for a back-up C2 Server.

48. The Glupteba Enterprise provides the C2 server information in an encrypted code in a transaction-specific message field on the Bitcoin blockchain. The message field is used to communicate messages or data from one Bitcoin address to another, similar to a check memo line, or the payment note in a digital payment application like Google Pay (*e.g.*, “for groceries”). The domain is either sent as a standalone, valueless data transmission, or accompanies a transaction in which funds are exchanged.

49. Thus, whenever a C2 server is taken offline, Glupteba malware is programmed to locate a replacement C2 server by querying the public blockchain, identifying transactions that involve the addresses controlled by the Glupteba Enterprise, and then decrypting the encrypted code contained in the message field of the relevant transaction in order to identify the back-up C2 server.

50. The Glupteba Enterprise’s use of blockchain technology to reinforce its C2 servers means the Glupteba botnet is particularly difficult to disrupt. Unlike conventional botnets, which may lose control of infected devices when a C2 server is shut down, the Glupteba botnet can continue to communicate instructions to its

infected devices even where domains for C2 servers are taken down, because the malware in the infected devices instructs the devices to identify a new C2 server by querying the blockchain. Thus, the Glupteba botnet cannot be eradicated entirely without neutralizing its blockchain-based infrastructure.

Criminal Schemes Perpetrated by the Glupteba Enterprise

51. The Glupteba Enterprise carries out several criminal schemes and facilitates the criminal schemes of others through its operation of the Glupteba botnet.

52. Each criminal scheme generates profits for the Glupteba Enterprise through illegal services. These schemes include: (1) stealing credentials of Google accounts (and other accounts) from infected devices and using that stolen account information for the Glupteba Enterprise's benefit, including by selling access to the stolen account to third parties through virtual machines preloaded with those accounts, minimizing the likelihood the account owners will detect the scheme, (2) selling credit cards to third parties to facilitate the fraudulent purchase of Google ads (and other Google services) that are never paid for, (3) selling the placement of disruptive ads on Glupteba-infected mobile devices, (4) selling proxy connections to infected devices, and (5) exploiting the processing power of infected devices to "mine" cryptocurrency.

53. **Stolen Accounts Scheme.** The Glupteba Enterprise harvests data that is maintained in internet browsers on infected devices, including data from Google Chrome and Google Ads. The stolen data includes confidential information belonging to the legitimate owner of the device, such as login credentials (usernames

and passwords), URL history, and authentication permissions (cookies). This stolen information is used in numerous ways to benefit the Glupteba Enterprise.

54. One way that the Glupteba Enterprise benefits from this stolen information is through the sale of *access* to stolen Google and similar accounts. The Glupteba Enterprise uses a website called “Dont.farm” to sell access to users’ accounts with Google and other online platforms.

55. The Enterprise loads stolen credentials and cookies of the stolen accounts on virtual machines. A virtual machine is similar to a physical computer, but the operating system of the virtual machine is contained within another computing environment, typically on a cloud computing platform.

56. Like typical computers, the Glupteba Enterprise’s virtual machines have a web browser. In the open browser, the Glupteba Enterprise enters a username and password for a Google account (or other account) that Glupteba malware has stolen. Dont.farm’s customers pay the Glupteba Enterprise in exchange for the ability to access a browser that is already logged into a victim’s stolen Google account. Once granted access to the account, the Dont.farm customer has free rein to use that account however they desire, including buying advertisements and launching fraudulent ad campaigns, all without the true account owner’s knowledge or authorization. According to Dont.farm’s website, customers can obtain access to “accounts of any country in the world.”

57. Dont.farm confesses that it is selling access to other people’s accounts for Google and other technology company products and services.

Invoice account

Buy a Google Ads account

Buying a Google Ads ad account from 3F will get an additional 1,350,000 VND to the account after 30 days of running the ad

Google Ads	Type 10\$	Google Ads	Type 50\$	Google Ads	Type 100\$
Money in the account	10\$	Money in the account	50\$	Money in the account	100\$
Give away promo code	1,350,000 VND	Give away promo code	1,350,000 VND	Give away promo code	1,350,000 VND
Can top up the budget	Yes	Can top up the budget	Yes	Can top up the budget	Yes
Refund if suspended	24h	Refund if suspended	12h	Refund if suspended	3h
Support account when suspended	slow	Support account when suspended	fast	Support account when suspended	fast
Need to pay	260,000 VND	Need to pay	1,300,000 VND	Need to pay	2,600,000 VND
Buy an account		Buy an account		Buy an account	



dont.farm

Russia

Category: [Accounts generator](#)

Site

We provide trusted Facebook accounts for successful advertising campaigns.

Account information:

- Accounts of real users only. Not a brute, not a farm. Real users only
- All of the accounts are at least 2 years old (most of them 5+ years)
- You connect to account via RDP. It takes less than a minute to launch your first campaign
- Accounts of any country of the world
- Only A++ class proxy which equals to the location of the user

Price includes the browser and the proxy. Everything is settled up an account is verified by phone

How it works:

- Your access to the account via RDP. Browser and proxy is build-in no additional expenses for it
- You can use only in this way, it is a guarantee that the account will live long.
- It takes less than a minute to start using the account

58. The Dont.farm website provides a manual instructing its users how to exploit accounts while minimizing the risk of discovery by the account owner or a technology platform like Google.

1. The first and the most important - never open letters, which are sent to user, use only google ads account, youtube (if necessary) and google analytics (if necessary). If you will follow this rule, you won't lose an account.

1.1. If you need to accept some invitation (for MCC, transfer audience or something else), then in search in email write: in:archive and find your letters.

2. Check the steps by file with notifications turning off and letters in email
https://docs.google.com/document/d/10YCV4KH-RLq187cnZ3Sf4uv0BLJ3OBWV0C2U6Hm_vpl/edit?usp=sharing

3. To register personal adwords account you can use this link
<https://ads.google.com/um/Welcome/Home?sf=bb&escape=expert&authuser=0&pli=1#ac>

4. When filling up billing info, take zip file from whoer.net, or if account's owner address information was filled in, then we skip this step.

5. When attaching payment method, choose Name and Surname of the account owner.

6. The first day launch the company only with white-hat offer, choosing a minimal daily limit on campaign and wait for the start of the campaign.

7. If after 2 days of campaign creation it is still not accepted - send the ticket about this problem to support via this link: https://support.google.com/google-ads/contact/approval_request
 As usual, the next day the campaign is getting approved and starts working, but any letter from support won't be received.

8. Then you can launch your blackhat campaigns. You can do it via new group of ads in the same campaign, or you can create a new ad campaign and add new group of ads.

Recommendations which you can implement, but not necessarily:

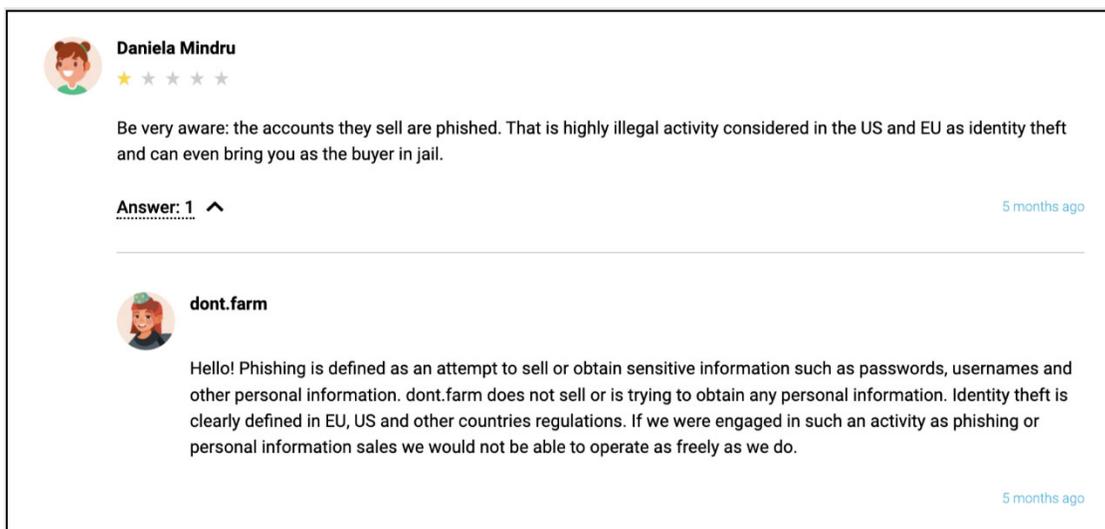
- for cloaking only no redirection method.
- don't use wordpress templates and wordpress itself - google doesn't like it.
- to protect your domain - use cloudflare.
- we recommend to use aged domains (from 2 weeks minimum, and as older the better)
- don't increase your budget immediately, on more than 30%

59. For example, Dont.farm customers are instructed to archive emails from “google.com” and “ads-reply@google.com” so that any alert emails from Google to the true owner of the account will not be noticed. Dont.farm customers also are instructed to turn off account notifications for Google AdWords and YouTube services so that the true owner of the account will not be notified of any changes made to their account.

60. Dont.farm also provides other tips to its customers to help them avoid detection by Google. For example, they advise customers not to increase advertising budgets by more than 30 percent, and that any domains used for advertisements should be at least two weeks old, if not significantly older.

61. According to the Dont.farm website, it has been in operation since 2019 and has over 200 employees. Dont.farm has sold access to hundreds of thousands of stolen accounts—including Google accounts—since its inception.

62. In response to a public comment accusing Dont.farm of illegal activity, Dont.farm attempted to distinguish its criminal conduct—selling authorized access to accounts—from the act of selling stolen username and passwords.



63. This is a distinction without a difference: while it is illegal to sell stolen usernames and passwords, it is likewise illegal to sell unauthorized access to a stolen account.

64. Dont.farm is marketed as a means by which to conduct “efficient” advertisement campaigns, but, in reality, it is simply a vehicle for bad actors to commit commercialized ad fraud. Once criminal customers are logged in to the victim’s account through Dont.farm, they can use the account to disseminate and/or purchase advertising. Cybercriminals often use this form of advertising to phish credentials, such as financial information or other personal information, from buyers

of their “products.” These bad actors may potentially use these accounts to conduct other fraudulent schemes as well.

65. With regard to the Stolen Accounts Scheme, Google specifically found the following through its investigation:

- a. Google identified a Gmail account sold by Dont.farm that was created in 2016. It did not initiate use of Google Ads until five years later, on April 21, 2021. On that same day, the account was logged into after four failed password attempts from an IP address in Germany, a location atypical of prior account logins. The very next day, on April 22, 2021, the account had logins from IP addresses tied to the United States and Iran. Review of these logins showed they occurred from a variety of device and browser types. In addition, a review of the Gmail settings on the account indicated it had established a filter to send all emails from “@google.com” to trash, consistent with the aforementioned instructions from Dont.farm.
- b. Google identified a Gmail account sold by Dont.farm that was created in 2018. It did not initiate use of Google Ads until three years later, on March 30, 2021. On that same day, the account was logged into from a new device. Google’s review determined that the Gmail settings on the account indicated it had established filters to send all emails from ads-account-noreply@google[.]com and from google[.]com to trash, consistent with Dont.farm’s instructions. Additionally, Google observed a series of

failed login attempts for this account in early July 2021 from IP addresses associated with numerous countries, such as Vietnam, Italy, Brazil, Ecuador, Iraq, Czechia, Bangladesh, and the United States.

- c. Google identified a Gmail account sold by Dont.farm that was created in 2019. It did not initiate use of Google Ads until two years later, on March 24, 2021. On that same day, the account was logged into from a Windows device in the United Kingdom, a device and location atypical of other logins, including another login that occurred that same day. The Gmail settings on the account indicated it had established filters to send all emails from ads-account-noreply@google[.]com and google[.]com to trash, consistent with Dont.farm's instructions.

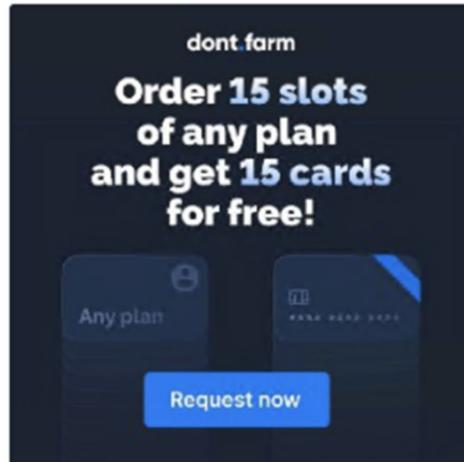
66. **Credit Card Fraud Scheme.** Often, third parties and potentially bad actors seek access to Google Ads accounts or similar advertising accounts to buy advertisements to display to Google users or other audiences. As reflected in images from the Dont.farm website excerpted below, one of the features of Dont.farm is that it offers “packages” that include not only access to stolen accounts, but also the use of credit cards from a website called Extracard.net to purchase ads. Customers of Dont.farm pay a fee for use of credit cards through Extracard.net; they use the card to purchase Google ads or other Google services (while logged in through stolen account information), but neither Extracard.net, nor the Dont.farm customer pay Google for the ads or services purchased.

Thursday, April 22, 2021



Promo | dont.farm admin

10:09:38 AM



Hurry up and get a FREE [extracard.net](#) CC for ordered [dont.farm](#) accounts!

Buy 15 slots of any package and get 15 bank cards as a gift!

What are [extracard.net](#) CCs:

- No documents needed!
- Card is issued in 5 minutes!
- Unique BIN only
- Each card is credit one and has a Platinum status!
- Full and easy access to 3ds and sms codes.

Please contact your manager for more information.

The action is until May 5 inclusive.

Construct an account suitable for you!

Advanced account

Facebook Account for running traffic.

- Unlimited usage
- A stable solution for Facebook issues
- Tier 1 Countries

\$700

Business Manager Warm-up

Ready to use (M)(x), allows you to run traffic right away.

- 3-5 Ads Accounts
- High spend limits

x2 **\$700**

Bank Card

Premium payment solution from [extracard.net](#).

- Perfect solution for Facebook and Google
- Real plastic cards (not virtual)
- A new experience when paying for ads and online purchases

\$200

Price:
\$1600

Discount:
\$51

Total cost:
\$1549

Purchase →

67. Specifically, the scheme leverages an advance credit Google provides to Google Ads account holders when an account holder places a credit card on file with their account. The account holder can spend up to the credit amount before Google charges the credit card on file. When account holders place legitimate credit cards on file, Google can collect the charges when it runs the credit card.

68. Extracard.net provides access to credit card numbers that are associated with a Russian bank. These credit card numbers appear legitimate, but when Google seeks to charge credit cards issued by Extracard.net, the charged amount is not fully paid. By taking advantage of the advance credit system, customers of Google Ads with Extracard.net credit cards on file have been able to “purchase” and execute ad campaigns without paying for them, causing monetary loss to Google. Additionally, many of the ad campaigns purchased with Extracard.net credit cards have been malicious or fraudulent.

69. The Glupteba Enterprise sells these credit cards through Extracard.net not just for use on its stolen Google accounts, but for the customer to use however they see fit. Thus, it is likely Google is not the only victim of this criminal scheme.

70. The Glupteba Enterprise directs and profits from this criminal scheme and operates the corporate entities responsible for executing the scheme. Prestige-Media LLC, a Delaware corporation owned and operated by the Glupteba Enterprise, owns QIP.ru, which claims responsibility for the creation and operation of Extracard.net. *See infra* paragraph 111.

71. With regard to the Credit Card Fraud Scheme, Google specifically found the following through its investigation:

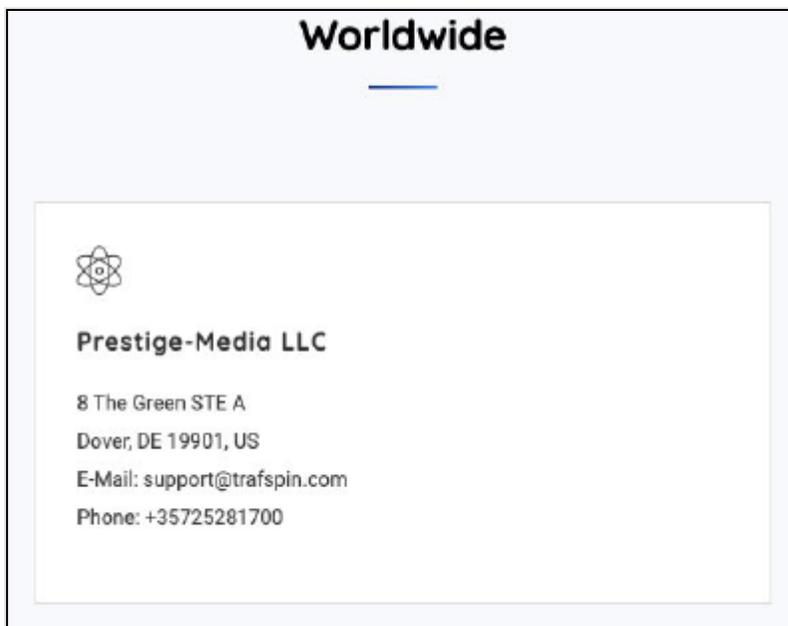
- a. The Google Ads accounts associated with a particular Gmail account purchased ads using a credit card consistent with credit cards from Extracard.net. Both Ads accounts were suspended for ad cloaking, a technique used to defraud online advertisers and trick internet users to view malicious sites, often with the purpose of compromising their devices. Upon review, the Ads accounts were found to be running ads which redirected to a cryptocurrency investment scam. Moreover, a review of that Gmail account indicated it had logins from IP addresses associated with AWMProxy.net.
- b. The Google Ads account associated with a particular Gmail account signed up for Google AdWords using a credit card consistent with credit cards from Extracard.net. The Ads account was suspended for payment fraud because it ran ads worth \$410.89 Australian Dollars in mid-September 2021, for which Google never received payment. This account was created just two weeks before it began using Google AdWords and it used VPN IP addresses for logging in, suggesting that the user purposefully masked its identity and likely created the account in order to undertake fraudulent ad activity using the Extracard.net credit card.

- c. The Google Ads account associated with a particular Gmail account signed up for Google AdWords using a credit card consistent with credit cards from Extracard.net. The account was suspended for payment fraud because it ran ads worth approximately 2800 EUR between June 4, 2021 and June 18, 2021, for which Google was only partially paid.

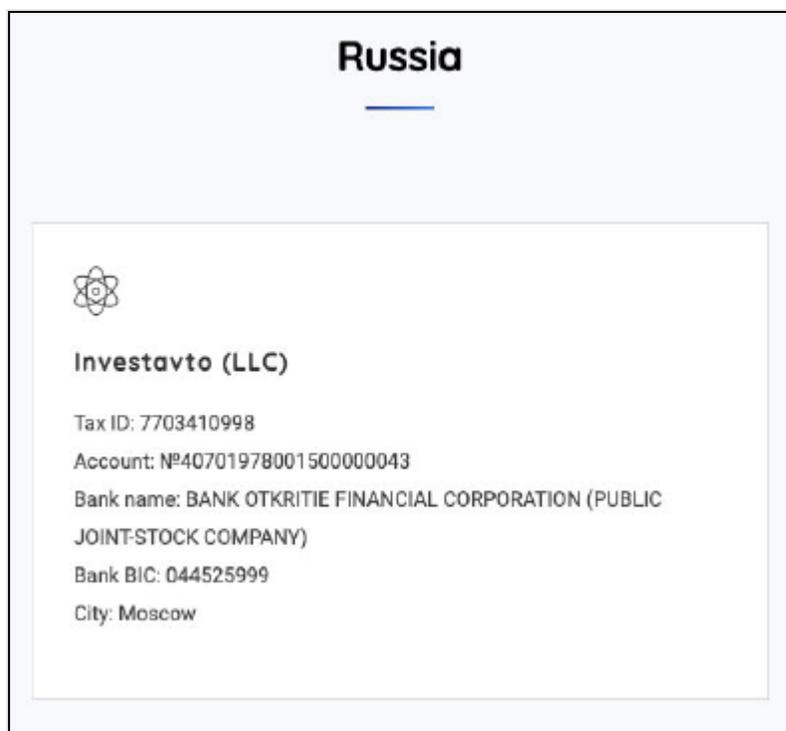
72. **Disruptive Ads Scheme.** The Glupteba Enterprise sells the placement of “disruptive ads” (often, “pop-up” ads) on mobile devices infected with malware. In today’s digital age, advertisers tend to view disruptive ads as more effective than standard ads used on social media and other websites because they grab users’ attention. The Glupteba Enterprise has sold disruptive ads through at least two websites, Trafspin.com and Push.farm.

73. Trafspin.com is a real-time bidding advertising network that sells disruptive in-app and web traffic through the botnet’s proxy connections to mobile devices infected by the Glupteba malware. Trafspin.com is currently offline, but it appears to have been replaced by Push.farm. The format and content of the Push.farm website is nearly identical to Trafspin.com, and it lists the same “office” phone number on its website.

74. Like Extracard.net, Trafspin.com and Push.farm appear to be supported by Prestige-Media. As shown below, Prestige-Media was listed on Trafspin.com’s website as the entity supporting Trafspin.com’s U.S. operations.



75. Similarly, as shown in the excerpt below from Trafspin.com's website, Trafspin.com and Push.farm's Russian operations appear to be supported by Investavto LLC, a Russian limited-liability company based in Moscow. Investavto was registered on May 26, 2016, and its legal address was 123112, Moscow, Presnenskaya Embankment 12, Office 5. Investavto may have been liquidated on September 23, 2021.



76. A third corporate entity supporting Trafspin and Push.farm is Valtron LLC (ООО БАЙТРОН in Russian), a Russian limited-liability company based in Moscow. It was incorporated on August 23, 2019. Recent Russian job postings state that Valtron LLC’s website is “Trafspin.com” and list the same office address as Voltronwork.com, Investavto LLC, and Trafspin.com: Presnenskaya Embankment 12 (Federation Tower). The job postings include requirements that the candidates have experience with Google and other technology-company advertising.⁸

77. **Proxy Scheme.** The Glupteba Enterprise also uses the botnet’s connections to infected devices to secretly convert those devices into proxy

⁸ The Glupteba Enterprise’s corporate entities likely exist for the sole purpose of hiring and paying employees. See Robert McMillan, *Ransomware Gang Masquerades as Real Company to Recruit Tech Talent*, Wall St. J. (Oct. 21, 2021, 8:30 AM), <https://www.wsj.com/articles/ransomware-gang-masquerades-as-real-company-to-recruit-tech-talent-11634819400>.

connections that it then sells to third-party customers, including those involved in criminal activity. Specifically, AWMPProxy.net⁹ sells residential proxy servers that allow customers (including criminals) to conceal their location through the use of devices infected by the botnet.

78. AWMPProxy.net rents out IP addresses that belong to physical devices infected by Glupteba malware to customers seeking to proxy (or relay) their internet activity through those devices. This enables customers to conceal their location, since their internet activity will appear to be coming from the IP address of the infected device, rather than the customers' real location. AWMPProxy.net updates the available proxies frequently in order to circumvent bans by search engine optimization.

79. IP addresses are a common factor used in identifying harmful activity, and by relaying efforts through residential proxies, bad actors are more likely to avoid detection and successfully undertake harmful activities such as launching malicious or fraudulent Google Ad campaigns and sending phishing emails to Google users. The unwitting victim owners whose devices have been infected are not aware, nor have consented, to their devices being used in this way.

⁹ On November 23, 2021, AWMPProxy.net was rebranded as Vd.net. A blog post on the same day claimed new ownership. *See The Project Has a New Domain and New Owners!*, VD.net (Nov. 23, 2021), <https://vd.net/news/the-project-has-a-new-domain-and-new-owners.html> (“Dear friends! We are glad to inform you that our project has been sold to new owners. In this regard, we expect new positive changes and you can already see the first one of them - we have a new website address! We are sure that the new team will breathe new life into the project!”).

80. The Glupteba Enterprise formerly used a website called “Abm.net” to effectuate the same scheme. Both AWMPProxy.net and Abm.net have advertised their proxies as compatible with Google.

81. AWMPProxy.net also provides proxy services for use by Dont.farm, as it appears that most of the IP addresses used to proxy for Dont.farm are IP addresses that AWMPProxy.net also utilizes.

82. The Glupteba Enterprise’s proxy scheme allows cybercriminals who rent an IP address from the Glupteba Enterprise to hide their tracks by concealing their true locations and IP addresses at the expense of unwitting and innocent owners of infected computers and devices. As a result, security systems that screen for suspicious IP addresses are less likely to detect the cybercriminal’s activity.

83. AWMPProxy.net and Abm.net also appear to be supported by Prestige-Media. All three share the same legal address (8 The Green, Suite A, Dover, Delaware, 19901), and AWMPProxy.net’s website previously listed Prestige-Media as a contact.

84. **Cryptojacking Scheme.** “Cryptojacking” involves secretly exploiting computing and processing power devices to generate or “mine” cryptocurrency.

85. For traditional, state-backed currencies (such as the U.S. dollar), new currency is injected into the economy when the government prints it. Cryptocurrency works differently, and for certain cryptocurrencies, newly issued currency is distributed to those who “mine” it. Specifically, cryptocurrency networks require confirmation of transactions. Transactions are confirmed by solving complex

mathematical problems (called “mining”) using computer processing power. After confirmation, transactions are confirmed to the blockchain. Miners are rewarded for being the first to successfully complete this computational task by receiving newly created units of cryptocurrency, often in the form of a “transaction fee.”

86. It is often not efficient or possible for the owner of a personal computer to “mine” cryptocurrency in this way.

87. The Enterprise manipulates infected devices, marshaling their collective computing power, to mine for cryptocurrency for the Glupteba Enterprise. The Enterprise directs all of the rewards from the mining activity to its own wallets, leaving the device owner both unaware that they are contributing to a criminal enterprise and saddled with the high electricity bill and computing inefficiencies that result from mining.

88. **Other Criminal Schemes:** As noted, the Glupteba malware has infected more than one million devices. At any moment, the unusual power of the botnet could be harnessed by the Glupteba Enterprise for any of a number of other criminal schemes, including large ransomware or DDoS attacks on legitimate businesses or targets of all sizes. The Glupteba Enterprise could itself perpetrate such a harmful attack, or it could sell access to the botnet to a third-party for such a purpose. Some of the largest DDoS attacks in internet history were recently carried

out by the so-called “Meris botnet,” which some researchers have connected to the Glupteba Enterprise.¹⁰

Developer Support for Criminal Schemes

89. The Glupteba Enterprise actively recruits developers to support its websites, transactions, and overall operation. To recruit developers, the Enterprise uses a website called “Voltronwork.com.” This site uses Google advertisements to post job openings for the websites effectuating the above criminal schemes.

90. Generally, Voltronwork.com has operated as a website that is central to the Glupteba Enterprise’s operations. An IP address once connected to vpn.voltronwork.com was used to login to Google accounts from domains associated with Dont.farm and AWMProxy.net. Additionally, advertisements from Voltronwork.com link to Trafspin.com, and the URL of a Voltronwork.com subdomain was visible in a 2020 variant of the Glupteba malware proxy module.

91. Voltronwork.com is no longer functioning, but it appears to have been replaced by Undefined.team, which the Glupteba Enterprise also controls and operates. The domain Undefined.team has been associated with Voltronwork.com since June 2021. Undefined.team shares the same Federation Tower address (Presnenskaya Embankment 12) as Voltronwork.com, Valtron LLC, Investavto LLC,

¹⁰ See Catalin Cimpanu, *Russian Security Firm Sinkholes Part of the Dangerous Meris DDoS Botnet*, The Record (Sept. 21, 2021), <https://therecord.media/russian-security-firm-sinkholes-part-of-the-dangerous-meris-ddos-botnet/> (“[I]t is currently unclear if the Glupteba gang built the Meris botnet themselves or if another group rented access to Glupteba-infected hosts to deploy the MikroTik module that eventually led to Meris’ creation.”).

and Trafspin.com. Additionally, a September 2021 job posting for an HTML coder stated that Extracard.net and Abm.net were projects of the “large IT team UNDEFINED.TEAM.”

Individual Defendants’ Roles in the Glupteba Enterprise

92. Each named Defendant controls and/or participates in the Glupteba Enterprise’s operations.

93. Defendants Dmitry Starovikov and Alexander Filippov each used one of the Glupteba botnet’s proxy C2 servers in executing the Terms of Service required to set up their Gmail addresses.

94. Defendant Dmitry Starovikov operates the Glupteba botnet and helps lead the criminal schemes of the Glupteba Enterprise. In addition to using the aforementioned IP address of a Glupteba botnet proxy C2 Server when signing up for a Gmail account, Dmitry Starovikov has an email account under the Voltronwork.com domain, and acts as an administrator for the Voltronwork.com Google Workspace account. Additionally, the secondary email address for the Google Workspace Voltronwork.com account, is an email containing Dmitry’s name under the Trafspin.com domain.

95. Defendant Alexander Filippov operates the Glupteba botnet and helps lead the criminal schemes of the Glupteba Enterprise. In addition to using the IP address of a proxy C2 Server when signing up for a Gmail account, Filippov has email accounts associated with the Google Workspace accounts related to Voltronwork.com, Dont.farm, and Undefined.team. Moreover, Filippov’s Undefined.team account lists

the Russian Federation Tower address as the billing address, which is used by many other entities in the Glupteba Enterprise, as discussed above.

Harm to Google, its Users, and the Public

96. The Glupteba Enterprise harms the owners of the devices that are infected with the malware, Google, and countless other persons and entities.

97. The owners of infected devices are harmed in numerous ways, including through the theft and use of their account information, unauthorized access and criminal misuse of their device, and potential subjugation to the criminal schemes of third parties.

98. The Glupteba Enterprise causes substantial harm to Google.

99. The Glupteba Enterprise causes financial loss to Google, including but not limited to the losses incurred in connection with the Credit Card Fraud Scheme, which results in the purchase of Google ads and services that are provided but never paid for.

100. The Glupteba Enterprise also harms Google's relationships with Google users: it has illicitly accessed and exploited thousands of Google users' accounts (as well as thousands of accounts belonging to other technology companies), disrupting these users' experiences with the Google platform.

101. The Glupteba Enterprise also harms Google itself by threatening the safety and security of Google's products, including Gmail, YouTube, and Google Ads.

102. The Glupteba Enterprise impairs the value of Google marks, including by tricking individuals into downloading Glupteba malware through a fake "YouTube

Downloader” website that deceived users into believing they were downloading a video from Google’s YouTube video sharing platform, impairing Google users’ confidence and trust in Google, its services, and its platforms.

103. The Glupteba Enterprise causes Google to expend substantial resources to detect, deter, and disrupt it, due to the threat the Glupteba Enterprise and its criminal schemes pose to the security of Google’s platform.

104. Beyond Google and Google users, the continued proliferation of malware on Google platforms harms the internet ecosystem as a whole.

CLAIMS FOR RELIEF

CLAIM 1

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

105. Google incorporates by reference each and every foregoing paragraph of the Complaint as if set forth in full.

106. At all relevant times, Google is a person within the meaning of 18 U.S.C. §§ 1961(3).

107. At all relevant times, Google is a “person injured in his or her business or property by reason of a violation of” RICO within the meaning of 18 U.S.C. § 1964(c).

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

The RICO Enterprise

109. The 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; namely, creating and controlling a vast botnet using Glupteba malware, and using that botnet to execute numerous criminal schemes that harm and threaten to continue to harm Google, its users, and the public more broadly. These schemes include the Stolen Accounts Scheme (*supra* ¶¶ 53-65), the Credit Card Fraud Scheme (*supra* ¶¶ 66-71), the Disruptive Ads Scheme (*supra* ¶¶ 72-76), the Proxy Scheme (*supra* ¶¶ 77-83), and the Cryptojacking Scheme (*supra* ¶¶ 84-87).

110. As described *supra* at paragraphs 92 through 95, the Defendants and their co-conspirators have organized their operation into a cohesive group with specific and assigned responsibilities and a command structure, operating in the United States and overseas, targeting and using victim devices in the United States. Over time, they have adapted their operations and schemes to changing circumstances, recruiting new members to and enlisting new devices in their operation, developing new malware modules, and expanding the scope and nature of their activities.

111. The Glupteba Enterprise, including named Defendants and their unnamed co-conspirators (Doe Defendants), controls and uses multiple corporate entities to effectuate its various criminal schemes. One such corporate entity is Prestige-Media LLC, a Delaware limited liability company that owns the domain, QIP.ru, that is responsible for Extracard.net (used with the Credit Card Fraud Scheme). Prestige-Media also supports Trafspin.com, the website used to facilitate

the Disruptive Ads Scheme. Another corporate entity controlled by the Glupteba Enterprise is Valtron LLC, a Russian entity that supports Trafspin.com.

112. The individual Defendants named herein—Dmitry Starovikov and Alexander Filippov—are each bot controllers involved in providing instructions to devices infected with the Glupteba malware, in furtherance of the criminal schemes alleged herein.

113. The Defendants and their co-conspirators constitute an association-in-fact enterprise within the meaning of 18 U.S.C. §§ 1961(4) and 1962(c): the Glupteba Enterprise. The members of the Glupteba Enterprise share the common purpose of developing and operating the Glupteba botnet worldwide, as set forth above.

114. At all relevant times, each of the Defendants were and are associated-in-fact with the Glupteba Enterprise and participated in the operation or management of the Glupteba Enterprise.

115. At all relevant times, the Glupteba Enterprise was engaged in, and its activities affected interstate and foreign commerce within the meaning of 18 U.S.C. § 1962(c).

Pattern of Racketeering Activity and Predicate Acts

116. At all relevant times, the Defendants conducted or participated, directly or indirectly, in the conduct, management, or operation of the Glupteba Enterprise's affairs 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.

117. Defendants have directly or indirectly engaged in an unlawful pattern of racketeering activity involving thousands of RICO predicate offenses including violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030(a)(5)(A), incorporated as a RICO predicate act under 18 U.S.C. § 1961(1)(G) and 18 U.S.C. § 2332b(g)(5)(B)); wire fraud (18 U.S.C. § 1343); identity fraud (18 U.S.C. § 1028); and access device fraud (18 U.S.C. § 1029). These activities have affected and continue to affect interstate or foreign commerce.

118. Google was injured in its business and property by reason of the Defendants' violations of 18 U.S.C. § 1962(c), as described herein. These injuries are a direct, proximate, and reasonably foreseeable result of these violations, and Google will continue to be harmed.

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

The Computer Fraud and Abuse Act Predicate Offenses

120. RICO provides, in 18 U.S.C. § 1961(1)(G), that any act indictable under 18 U.S.C. § 2332b(g)(5)(B) constitutes a RICO predicate act. Among the acts that are indictable under 18 U.S.C. § 2332b(g)(5)(B) are violations of 18 U.S.C. § 1030(a)(5)(A)—a provision of the Computer Fraud and Abuse Act (CFAA)—if such violation results in damage as defined in Section 1030(c)(4)(A)(i)(VI).

121. Defendants have violated and continue to violate the CFAA, 18 U.S.C. § 1030(a)(5)(A), resulting in damage as defined in Section 1030(c)(4)(A)(i)(VI), by infecting protected computers with malware, transmitting programs designed to

carry out their schemes, and transmitting commands to infected computers. Each of these violations constitutes a separate RICO predicate offense.

122. *Transmission of Malware “Droppers.”* Defendants have intentionally caused damage to “protected computers” by transmitting malware “droppers” to those computers, thereby impairing the integrity of their systems and information, and allowing Defendants to access those systems. The infected computers are “protected computers” within the meaning of the CFAA because they are used in or affect interstate commerce or communication through the internet. Through this conduct, Defendants have caused damage to 10 or more protected computers in a one-year time period.

123. *Transmission of Malware Modules.* Defendants have transmitted malware modules to protected computers through the internet. Those modules damage the protected computers by disabling the users’ cybersecurity detection tools, anti-virus software, and system monitoring programs, as well as transmitting other modules to execute Defendants’ criminal schemes. Through this conduct, Defendants have caused damage to 10 or more protected computers in a one-year time period.

124. *Transmission of Commands.* Defendants also have transmitted commands to protected computers through the internet, thereby causing damage to those computers and enabling the Glupteba Enterprise to utilize these computers in its criminal schemes. Through this conduct, Defendants have caused damage to 10 or more protected computers in a one-year time period.

125. Google has suffered injury to its business or property as a result of these predicate offenses, including due to Defendants' use of these violations in furtherance of the Stolen Accounts and Credit Card Fraud Schemes.

Wire Fraud Predicate Offenses

126. 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 in three ways, each instance of which constitutes a separate RICO predicate offense.

127. First, the Glupteba Enterprise commits wire fraud, in violation of 18 U.S.C. § 1343, each time that it tricks the owner of a device into unknowingly downloading and installing Glupteba malware on the owner's device through fraud, misrepresentation, and deception. For example, the Glupteba Enterprise misused a known Google mark, YouTube, described *supra* at paragraphs 33 and 102, which constitutes an act of wire fraud, in violation of 18 U.S.C. § 1343.

128. Second, in connection with the Stolen Accounts Scheme, Defendants steal Google users' login information (*e.g.*, usernames and passwords), and then sell access to open browsers that are pre-loaded with the stolen login information, thereby deceiving Google through deceit and false pretenses as to the true identity of the person accessing the Google account. Each time that the Glupteba Enterprise

facilitates an unauthorized login to a Google user's account by a person other than the true Google user, for the purpose of obtaining money or property, including as described *supra* at paragraphs 53 through 65, the Glupteba Enterprise commits an act of wire fraud, in violation of 18 U.S.C. § 1343.

129. Finally, the Glupteba Enterprise commits wire fraud through the Credit Card Fraud Scheme. The Glupteba Enterprise deliberately markets credit cards through Extracard.net and markets those cards specifically for use to purchase ads fraudulently on Google or other Google services, knowing that the cards can be used in connection with fraudulent activity. The Glupteba Enterprise's customers can use these cards to purchase Google Ads, falsely representing to Google that the cards are fully funded. The Glupteba Enterprise causes these transmissions because the Enterprise knows the transmissions can follow in the ordinary course of business and such use can reasonably be foreseen.

130. Google has suffered injury to its business or property as a result of these fraudulent schemes.

Identity Fraud Predicate Offenses

131. Defendants commit identity fraud in violation of 18 U.S.C. § 1028(a)(7) by knowingly transferring, possessing, and using, without lawful authority, means of identification of their victims with the intent to commit, or to aid or abet, or in connection with, unlawful activity in violation of state and federal law and affecting interstate commerce.

132. Specifically, in connection with the Stolen Accounts Scheme and the Credit Card Fraud Scheme, the Glupteba Enterprise transfers, possesses, and uses, without authorization, the usernames and passwords of users whose account information has been stolen. Those usernames and passwords are “means of identification” because they belong to and identify specific individuals. The Glupteba Enterprise acts with the intent to commit unlawful activities that violate federal law (including the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(A), and 18 U.S.C. § 1343) and that constitute felonies under state law (including theft of property).

133. Google has suffered injury to its business or property as a result of these actions.

Access Device Fraud Predicate Offenses

134. Defendants, knowingly and with intent to defraud, committed and continue to commit access device fraud in violation of 18 U.S.C. § 1029(a)(2) and (3) by trafficking in or using unauthorized access devices in the form of stolen passwords, credentials, and other account information in order to obtain anything of value aggregating \$1,000 or more during a one-year period, and/or possessing fifteen or more unauthorized access devices, and affecting interstate or foreign commerce.

135. For instance, the Glupteba Enterprise loads stolen usernames and passwords and cookies onto virtual machines, and then sells access to stolen Google accounts (and the accounts of other technology companies). Each set of credentials in a virtual machine is an “unauthorized access device” because it is a means of

accessing a user's account and was stolen by the Glupteba Enterprise. The Enterprise possesses thousands of unauthorized access devices, which it has obtained during a one-year period.

136. Google has suffered injury to its business or property as a result of these actions, which the Glupteba Enterprise uses to carry out the Stolen Accounts and Credit Card Fraud Schemes.

Conspiracy to Violate RICO

137. Google incorporates by reference each and every foregoing paragraph of the Complaint as if set forth in full.

138. 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).

139. The Defendants knew that they were engaged in a conspiracy to commit multiple predicate offenses, and they knew that the predicate offenses were part of such racketeering activity, and their participation and agreement was necessary to allow the commission of 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).

140. The Defendants agreed to direct or participate in, directly or indirectly, the conduct, management, or operation of the Glupteba Enterprise's affairs through

a pattern of racketeering activity in violation of 18 U.S.C. § 1962(c). Each Defendant knew about and agreed to facilitate the Glupteba Enterprise's schemes. The purpose of the conspiracy was to commit a pattern of racketeering activity in the conduct of the affairs of the Glupteba Enterprise, including the acts of racketeering set forth above.

141. 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.

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

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

CLAIM 2
Violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030

144. Google incorporates by reference each and every foregoing paragraph of the Complaint as if set forth in full.

145. Defendants intentionally accessed and continue to access protected computers without authorization and thereby obtained and continue to obtain information from the protected computers. *See* 18 U.S.C. § 1030(a)(2)(C). The protected computers include devices infected with Glupteba malware, from which Defendants obtain information concerning the device's owner, including usernames and passwords. The protected computers also include Google's servers, which

Defendants intentionally accessed without authorization to obtain information from Google concerning the account, and use of the account.

146. Further, as described above at paragraphs 29 through 40, Defendants knowingly caused and continue to cause the transmission of a program, information, code, and/or commands, and as a result of such conduct, intentionally caused and continue to cause damage without authorization, to the protected computers, the software residing thereon, and Google. *See* 18 U.S.C. § 1030(a)(5)(A).

147. Defendants intentionally accessed and continue to access protected computers without authorization, and as a result of such conduct, recklessly caused and continue to cause damage to the protected computers, the software residing thereon, and Google. *See* 18 U.S.C. § 1030(a)(5)(B).

148. Defendants intentionally accessed and continue to access protected computers without authorization, and as a result of such conduct, caused and continue to cause damage and loss to the protected computers, the software residing thereon, and Google. *See* 18 U.S.C. § 1030(a)(5)(C).

149. Defendants knowingly and with intent to defraud trafficked and continue to traffic in passwords and/or similar information through which computers may be accessed without authorization. *See* 18 U.S.C. § 1030(a)(6).

150. Defendants' conduct involved and affected, and continues to involve and affect, interstate and/or foreign communications and commerce, including involving protected computers located inside the United States as well as protected computers

located outside the United States that are used in a manner that affects interstate or foreign commerce or communication of the United States.

151. Defendants' conduct has caused damage to Google, including by impairing the integrity of the accounts being offered to certain of its users.

152. Defendants' conduct has caused a loss to Google during a one-year period aggregating at least \$5,000

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

154. 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.

CLAIM 3
Violations Of The Electronic Communications Privacy Act, 18 U.S.C. §§
2701 *et seq.*

155. Google incorporates by reference each and every foregoing paragraph of the Complaint as if set forth in full.

156. Google accounts and Google's servers running such services are facilities through which electronic communication service is provided to Google users and customers.

157. Defendants knowingly and intentionally accessed and continue to access Google accounts and Google's servers running such services without authorization or in excess of any authorization granted by Google or any other party.

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

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

CLAIM 4
Trademark And Unfair Competition Violations

160. Google incorporates by reference each and every foregoing paragraph of the Complaint as if set forth in full.

161. Since Google's founding in 1997, its search engine, accessible at www.google.com, has become one of the largest, most recognized, and widely used internet search services in the world.

162. Among its innovative goods and services, Google also offers a video sharing service under the famous YOUTUBE mark. YouTube, LLC ("YouTube") launched the youtube.com website on April 24, 2005, and the mark YOUTUBE has been in continuous use ever since. Google acquired YouTube in November 2006, and thereafter maintained YouTube's rights and use of the YOUTUBE mark.

163. Google has devoted substantial efforts and resources, both in the United States and internationally, to promote its services using its trademarks including YOUTUBE. Its platforms have had resounding success in the marketplace and have garnered a significant and loyal network of users, including consumers, advertisers and content providers. Today, these platforms are among the most used services in their fields and the most visited websites and apps in the world.

164. Google owns numerous trademark registrations in the U.S. and around the world for its marks including YOUTUBE, including but not limited to

incontestable U.S. Trademark Reg. No. 3711233, registered in 2009 and renewed in 2020, covering the following goods and services:

(Int'l Class: 09)

Downloadable software to enable uploading, posting, showing, displaying, tagging, sharing and otherwise providing electronic media or information over the Internet and other communications networks; application program interface (API) that enables developers to integrate video content and functionality into websites, software applications, and devices

(Int'l Class: 35)

Advertising and promotional services on behalf of others; promotional services, namely, promoting the goods and services of others through online entertainment, online education, and sharing of multimedia content via the Internet and other communications networks; developing and providing marketing programs for advertisers, marketers, and content providers; providing a website where advertisers, marketers, and content providers can reach, engage, and interact with online users for the purposes of promotion or advertising

(Int'l Class: 38)

Audio, video and multimedia broadcasting via the Internet and other communications networks; webcasting services; transmission of messages, data and content via the Internet and other communications networks; providing forums for the transmission of messages, comments and multimedia content among users in the field of general interest via

the Internet and other communications networks; transmission of electronic media, multimedia content, videos, movies, pictures, images, text, photos, user-generated content, audio content, and information via the Internet and other communications networks; providing community forums for users to post, search, watch, share, critique, rate, and comment on, videos and other multimedia content via the Internet and other communications network

(Int'l Class: 41)

Entertainment and educational services, namely, providing a website featuring user-generated content, namely, electronic media, multimedia content, videos, movies, pictures, images, text, photos, audio content, and related information via the Internet and other communications networks on a wide variety of topics and subjects; Providing online journals, namely, blogs featuring information on the subject of the above-listed user-generated website content; Online digital video, audio and multimedia entertainment publishing services; Online digital publishing services; Entertainment services, namely, conducting contests

(Int'l Class: 42)

Providing temporary use of non-downloadable software to enable uploading, capturing, posting, showing, editing, playing, streaming, viewing, previewing, displaying, tagging, sharing, manipulating, distributing, publishing, reproducing, and otherwise providing

electronic media, multimedia content, videos, movies, pictures, images, text, photos, user-generated content, audio content and information via the Internet and other communications networks; Providing temporary use of non-downloadable software to enable sharing of multimedia content and comments among users; Providing temporary use of non-downloadable software to enable content providers to track multimedia content; Providing temporary use of non-downloadable analytics software, namely, software that provides statistics about the behavior of viewers of online videos, movies, pictures, images, text, photos, games and other user-generated content; Hosting of websites featuring multimedia content for others; Hosting multimedia entertainment and educational content for others; Providing a web site that gives computer users the ability to upload and share user-generated videos, on a wide variety of topics and subjects

165. Google's trademarks including YOUTUBE embody the substantial and valuable reputation and goodwill that Google has earned in the marketplace for its high-quality and innovative services and related software and products. In particular, the YOUTUBE brand has become famous because of, among other reasons, Google's widespread use of the mark in the United States and internationally, extensive media coverage, and the strong and loyal base of users of this Google service.

166. The YOUTUBE Mark was used by Defendants and/or their agents in connection with a domain name and website purporting to be a YouTube video downloader program that tricked the user into clicking the download link, infecting the user's computer with Glupteba malware and enabling Defendants to control the user's computer via instructions sent by Defendants' C2 server, as noted above. The fake YouTube video downloader is one of the nefarious means Defendants or their agents have used to gain access to users' computers and infect computers with the Glupteba malware.

167. Defendants thus in part access user accounts through malicious freeware that was marketed using the YOUTUBE Mark, purporting to offer YouTube video download programs and using the YOUTUBE Mark in domain names such as video-youtube-get.ru.

168. Defendants used the YOUTUBE mark in commerce in connection with the distribution and advertising of services in a manner that is likely to cause confusion.

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

169. Google incorporates by reference each and every foregoing paragraph of the Complaint as if set forth in full.

170. Defendants' and/or their agents' use of the YOUTUBE mark has caused and/or is likely to continue to cause confusion with Google's federally registered YOUTUBE trademark, in violation of 15 U.S.C. § 1114(1). The use by Defendants and/or their agents of YOUTUBE 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.

171. 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 YOUTUBE trademark.

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

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

173. Google incorporates by reference each and every foregoing paragraph of the Complaint as if set forth in full.

174. Defendants' and/ or their agents' use of YOUTUBE has caused and/or is likely to cause confusion in violation of 15 U.S.C. § 1125(a). Defendants' and/or their agents' use of YOUTUBE 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.

175. 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 YOUTUBE trademark.

***Federal False Advertising in Violation of the Lanham Act
15 U.S.C. § 1125(a)***

176. Google incorporates by reference each and every foregoing paragraph of the Complaint as if set forth in full.

177. 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).

178. Defendants' and/or their agents' advertising claims regarding alleged services offered by Defendants, including offering of software that purported to assist in downloading of videos from YouTube, have been false, deceptive, and misleading.

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

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

181. 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.

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

183. 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.

184. 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.

185. 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.

CLAIM 5
Tortious Interference with Business Relationship

186. Google incorporates by reference each and every foregoing paragraph of the Complaint as if set forth in full.

187. Defendants knew or should have known that Google had an actual and continuing business relationship with numerous users who interact with Google's systems and computer networks.

188. In violation of the common law of New York, Defendants intentionally and maliciously interfered with Google's business relationships with its users by accessing, without authorization, Google user accounts, and Google's systems and networks, for the purpose of stealing account information and data from those users, thereby causing harm to Google users, Google, and Google's relations with its users.

189. Moreover, Defendants unlawfully and maliciously interfered with Google's business relationship with prospective users by undermining the security and reputation of Google's systems and networks.

190. Defendants' improper actions were the proximate cause of harm to Google.

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

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

CLAIM 6
Unjust Enrichment

193. Google incorporates by reference each and every foregoing paragraph of the Complaint as if set forth in full.

194. The acts of Defendants complained of herein constitute unjust enrichment of the Defendants at the expense of Google in violation of the common law of New York. Defendants accessed, without authorization, Google's Gmail system and the computers by which such programs and services run.

195. Defendants profited unjustly from their unauthorized use of Google's systems and networks.

196. Defendants had an appreciation and knowledge of the benefit they derived from their unauthorized use of those systems and networks.

197. Retention by the Defendants of the profits they derived from their malfeasance would be inequitable.

198. Google seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial, including without limitation disgorgement of Defendant's ill-gotten profits.

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff 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 Racketeer Influenced and Corrupt Organizations Act, Computer Fraud and Abuse Act, Electronic Communications Privacy Act, and Lanham Act, and they have engaged in tortious interference with business relationships and been unjustly enriched;
- C. A declaration that Defendants have violated Google's trademarks;
- D. A declaration that Defendants' conduct has been willful and that Defendants have acted with fraud, malice, and oppression;
- E. 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;

- F. Award of appropriate equitable relief available under applicable statutes and law, including injunctive relief and an accounting of profits;
- G. 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;
- H. Judgment awarding enhanced, exemplary and special damages, in an amount to be proved at trial;
- I. Judgment awarding attorneys' fees and costs; and
- J. Order such other relief that the Court deems just and reasonable.

DEMAND FOR JURY TRIAL

Google respectfully requests a trial by jury on all triable issues in accordance with Fed. R. Civ. P. 38.

DATED: December 2, 2021

Respectfully submitted,

Laura Harris
Andrew Michaelson
Kathleen E. McCarthy
Matthew Bush
KING & SPALDING LLP
1185 Ave. of the Americas, 34th Floor
New York, NY 10036
Telephone: (212) 790-5356
Fax: (212) 556-2222
lharris@kslaw.com
amichaelson@kslaw.com
kmccarthy@kslaw.com
mbush@kslaw.com

Sumon Dantiki (*pro hac vice* to be submitted)
David P. Mattern (*pro hac vice* to be submitted)
KING & SPALDING LLP
1700 Pennsylvania Ave., NW, 2nd Floor
Washington, DC 20006
Telephone: (202) 626-5591
Fax: (202) 626-3737
sdantiki@kslaw.com
dmattern@kslaw.com

Bethany L. Rupert (*pro hac vice* to be submitted)
KING & SPALDING LLP
1180 Peachtree Street, NE, Suite 1600
Atlanta, GA 30309
Telephone: (404) 572-3525
Fax: (404) 572-5100
brupert@kslaw.com

Counsel for Plaintiff Google LLC