ATTORNEY-CLIENT PRIVILEGE
NEED-TO-KNOW

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

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

COMPLAINT FOR DAMAGES AND INJUNCTIVE RELIEF

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

INTRODUCTION

1. The scam begins with a text message. It may alert you to a problem with the delivery of a package and invite you to click a link to correct your address and pay a small delivery fee. Or it may warn you of an unpaid toll or ticket, directing you to a toll collection website that appears legitimate to pay the outstanding charges.

2. Or perhaps you see an online advertisement promising, for example, a low price for a popular, name-brand water bottle, and directing you to an e-commerce website where you can pay by credit card or Google Pay.

3. Millions of Americans have received these text messages and seen these ads, clicked on the link to a fraudulent website, entered payment and other personal information, and thereby became victims of the criminal scheme at the heart of this Complaint.[1] Google is seeking an injunction to disrupt the criminal enterprise behind this scheme and stop its spread.

4. The Defendants are a group of foreign cybercriminals who have engaged in relentless phishing attacks against millions of innocent victims, including Google customers, to steal personal and financial information. These attacks have collectively swindled innocent victims out of millions of dollars and harmed Google through the unauthorized use of its trademarks and services.

5. The key to Defendants' phishing attacks is a powerful phishing software kit called "Lighthouse."[2] Defendants created Lighthouse to serve as a "phishing for dummies" kit for

[1] *See* Consumer Alert, *Think that text message is from USPS? It could be a scam*, Fed. Trade Comm'n Consumer Advice (Apr. 23, 2025), https://tinyurl.com/2wr6vftd.

[2] As explained in more detail below, Phishing-as-a-Service or "PhaaS" has transformed phishing software into a business. Cybercriminals sell their phishing software alongside additional support services to facilitate the execution of increasingly sophisticated phishing schemes.

cybercriminals who could not otherwise execute a large-scale phishing campaign. For a monthly licensing fee, criminals can select either an SMS or e-commerce version of the software that includes hundreds of templates for fake websites, domain set-up tools for those fake websites, and other features designed to dupe victims into believing they are entering sensitive information on a legitimate website (the "Lighthouse Schemes" or "Schemes"). The templates are designed to mimic trusted institutions—like government entities, financial institutions, and postal services—to leverage the public's confidence in such institutions.

6. The scale of Lighthouse phishing attacks is staggering. In a 20-day period, approximately 200,000 fraudulent websites created using Lighthouse were used to attract "well over 1,000,000 potential victims" in at least 121 countries.[3] Lighthouse was used to launch 32,094 distinct United States Postal Service ("USPS") phishing websites from July 2023 through October 2024; between 12.7 million and 115 million credit cards may have been compromised in the United States alone.[4] Lighthouse-supported phishing websites have received an average of 50,000 page visits per day.

7. Although the software simplifies the creation of phishing websites, executing large-scale phishing attacks still requires coordination and cooperation among multiple actors. Some specialize in collecting contact information of potential targets, others focus on the logistics of sending SMS messages in bulk, and still others help to sell victims' stolen information. The members of these groups, along with the developers of Lighthouse and those

---

[3] *See Smishing Triad: Chinese eCrime Group Targets 121+ Countries, Intros New Banking Phishing Kit*, Silent Push Blog (Apr. 10, 2025), https://tinyurl.com/4m64c7pw. Some security firms use the term "Smishing Triad" to refer broadly to Wang Duo Yu and other China-based phishing-as-a-service software developers, but Silent Push's research focused on the Lighthouse software.

[4] *See Research: The Evolution of Chinese Smishing Syndicates and Digital Wallet Fraud*, SecAlliance (Aug. 5, 2025), https://tinyurl.com/ym4wwxhd.

who license the software to carry out attacks, are referred to herein as the "Lighthouse Enterprise" or the "Enterprise." The Enterprise created and maintains an online community of discussion forums that are used to plan and execute Lighthouse phishing attacks and recruit new members. There, Enterprise members market and sell Lighthouse, train members to use the software, and improve the operation's efficiency.

8. In facilitating and executing these phishing campaigns, the Lighthouse Enterprise preys on the public trust in Google, a leader in the technology space, by misappropriating Google branding, including by using Google logos on fraudulent websites. The Lighthouse Enterprise also 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 products and services, and forces Google to devote substantial resources to investigate and combat the Lighthouse Enterprise's criminal activity.

9. Disrupting the Lighthouse Enterprise will require persistence, because the Enterprise can execute new phishing schemes with little effort, thanks to the Lighthouse software and coordination on Lighthouse discussion forums. As the Enterprise detects threats to its infrastructure, it adapts its tactics and can shift its servers and domains within a matter of hours.

10. Google brings this action under the Racketeer Influenced and Corrupt Organizations Act ("RICO"), the Lanham Act, and the Computer Fraud and Abuse Act ("CFAA") to disrupt the Lighthouse Schemes, to prevent the Enterprise from causing further harm, and to recover damages.

PARTIES

Plaintiff

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

12. Google is a leading technology company that offers a wide variety of services to organize the world's information and make it universally accessible and useful. Its search engine, accessible at www.google.com, is the most widely used internet search service in the world. Gmail, a free email service used by more than 1.5 billion people worldwide, includes a variety of revolutionary and innovative features, including an industry-leading two full gigabytes of email storage; email message threading; fast, precise search of emails using an integrated Google search engine; and freedom from pop-up or irrelevant advertising. Google also offers YouTube, an online video sharing platform that millions of people use to share and watch videos each day.

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

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

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

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

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

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

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

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

h. **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.

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

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

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

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

Defendants

15. Defendants Does 1–25 are individuals or entities who have conspired to engage in a pattern of racketeering activity. They have each participated in the management or operation of the Lighthouse Scheme and engaged in criminal acts that have caused harm to Google, its users, and countless others. Upon information and belief, Defendants are based in China.

16. At this time, Google does not know the true names and capacities of the Doe Defendants sued as Does 1–25. Each of the Doe Defendants is responsible in some manner for the conduct alleged, having agreed to become part of the Lighthouse Enterprise.

17. Google is presently aware of several connected Doe threat actor groups within the Lighthouse Enterprise. It is not clear how many threat actors compose each group nor how many groups comprise the Lighthouse Enterprise; the Doe numbers are meant to be representative. These threat actor groups use overlapping infrastructure and interact to support and develop the Enterprise's criminal schemes. The groups—whose precise numbers and composition are not known—and their misconduct are described in more detail below.

JURISDICTION AND VENUE

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

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

20. Defendants have affirmatively directed actions at the United States, including the Southern District of New York, by creating fake websites mimicking the New York City government website (nyc.gov) and New York E-ZPass website (e-zpassny.com), among many others, for use in these phishing schemes. Defendants aimed illegal activities at individuals within the Southern District of New York.

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

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

FACTUAL ALLEGATIONS

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

23. As personal devices and email have replaced telephone lines and traditional mail, criminal activity has evolved and is leveraging those tools to reach more victims with less effort. One of the most common forms of internet-based criminal activity is phishing. The sophistication and reach of these schemes have grown dramatically—cybercriminals are now sending an estimated 3.4 billion phishing emails every day.[5] It has become the most ubiquitous form of criminal fraud.

24. "Phishing" is a type of cyberattack in which threat actors trick individuals into disclosing sensitive information like passwords, credit card numbers, or banking information,

[5] Sienna Arellano & Ian Kilty, *The Phishing Business Model*, Colo. State Univ. System: Info. Tech. (Feb. 17, 2025), https://tinyurl.com/psxum3se.

often by impersonating well-known brands, government agencies, or even people the victim knows. The attacker typically targets individuals with emails, text messages, or through fake advertisements that are designed to appear trustworthy. The phishing message asks the target to click a link or fill out a form to transmit personal data that the threat actors then steal for criminal use.

25. Short Message Service ("SMS") phishing scams (or, "smishing") refer to phishing attempts sent through text message or other telephone messaging services like RCS and iMessage. These messages, which can target thousands of phone numbers at a time, encourage recipients to click on a malicious link that leads to a fraudulent phishing website. The fake websites frequently mimic those of legitimate institutions such as toll enforcement agencies, postal and shipping companies, or financial institutions.

26. E-commerce phishing scams involve the creation and deployment of websites that purport to sell products but instead serve the primary purpose of collecting credit card details and other information for fraudulent uses. These websites mimic legitimate retail websites. Scammers direct customers to these websites through advertisements on social media platforms, search engines, or by sending email messages.

27. Once threat actors have victims' sensitive information in hand, they can use it to access email accounts, bank accounts, and more. Scammers often load stolen payment card information onto digital wallets—like Google Wallet—on mobile devices and then sell the devices to others to make unauthorized purchases. Scammers can also relay new stolen card information in real time to co-conspirators to make in-person purchases, a practice known as "ghost tapping."[6] Some recent law enforcement actions have identified criminal networks using

[6] Insikt Grp., *Ghost-Tapping and the Chinese Cybercriminal Retail Fraud Ecosystem*, Recorded Future: Cyber Threat Analysis (Aug. 14, 2025), https://tinyurl.com/3z9sa9jk.

phones loaded with stolen credit card information and tap-to-pay functionality to purchase gift cards in bulk.[7] Other groups simply purchase their own tap-to-pay machines or rely on a mobile app that allows them to use stolen cards on tap-to-pay machines, and use customer cards to make payments directly to themselves.[8] Still others use stolen brokerage firm credentials to perpetrate a modern iteration of a "pump and dump" scheme, pre-purchasing shares of a particular stock, and then using compromised brokerage accounts to purchase large volumes of the stock, inflating the price before they liquidate their original holdings.[9]

28. These schemes have proven to be so profitable that the infrastructure necessary to execute them has become a commodity. So-called phishing-as-a-service ("PhaaS") is a business model that sells software and support services to facilitate phishing, making it relatively easy for those without technical expertise to create a phishing campaign. The software, sometimes referred to as a "phishing kit," provides the infrastructure necessary to create a fake website (or other platform), send bulk text messages and emails to victims, and collect and store stolen personal and/or financial information. For example, a phishing kit may contain ready-made website templates that closely resemble legitimate websites. Phishing kits enable criminals without technical expertise to engage in phishing and smishing, to reach larger numbers of targets, and to mimic a greater number of websites, making these types of attacks much more nimble and ultimately more frequent.

---

[7] Josh Jarnagin, *Knox County detectives investigating 'ghost tap' credit card fraud*, WVLT8 (May 31, 2025), https://tinyurl.com/43rc82pu; *see also* Media Release: *Joint Advisory on Unauthorised Card Transactions Made Using Contactless Payment Methods in Singapore*, Monetary Auth. of Singapore (Feb. 17, 2025), https://tinyurl.com/3uabmj63.

[8] *See* Brian Krebs, How Phished Data Turns into Apple & Google Wallets, KrebsOnSecurity (Feb. 18, 2025), https://tinyurl.com/32arezcj.

[9] *See* Brian Krebs, Mobile Phishers Target Brokerage Accounts in 'Ramp and Dump' Cashout Scheme, KrebsOnSecurity (Aug. 15, 2025), https://tinyurl.com/532xpfwf.

29. The PhaaS model also makes it difficult to stop phishing attacks. "Catching the person who carried out the attack does not put an end to the story. You will still have to catch the guy who designed the phishing kit and the one who provided it."[10]

30. This ease of use also makes PhaaS an ideal vehicle to fund other criminal operations. For example, drug cartels use phishing to "expand their revenue streams and exert influence beyond traditional drug trafficking." The mafia uses phishing schemes to support their traditional offline activities.[11]

The Lighthouse Software

31. Members of the Enterprise market two versions of Lighthouse software. The first is the "SMS" version, for smishing. The second is the "e-commerce" version.

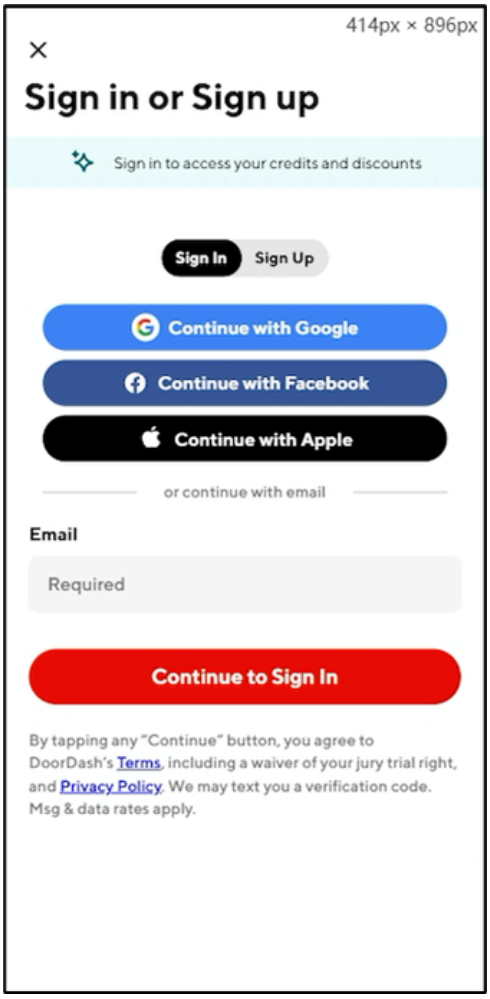
32. ***The SMS Version.*** The SMS version of Lighthouse enables scammers to distribute mass text messages to thousands of targets, directing them to fake websites (created using Lighthouse templates) where the victims are duped into providing personal and financial information.

33. Lighthouse offers over 600 templates for fraudulent phishing websites each designed to resemble the legitimate website of one of more than 400 entities or institutions. Lighthouse users can filter and search for templates by geographic region, country, official website, and update time. At least 116 templates feature a Google logo (YouTube, Gmail, Google, or Google Play) on the sign-in screen.

---

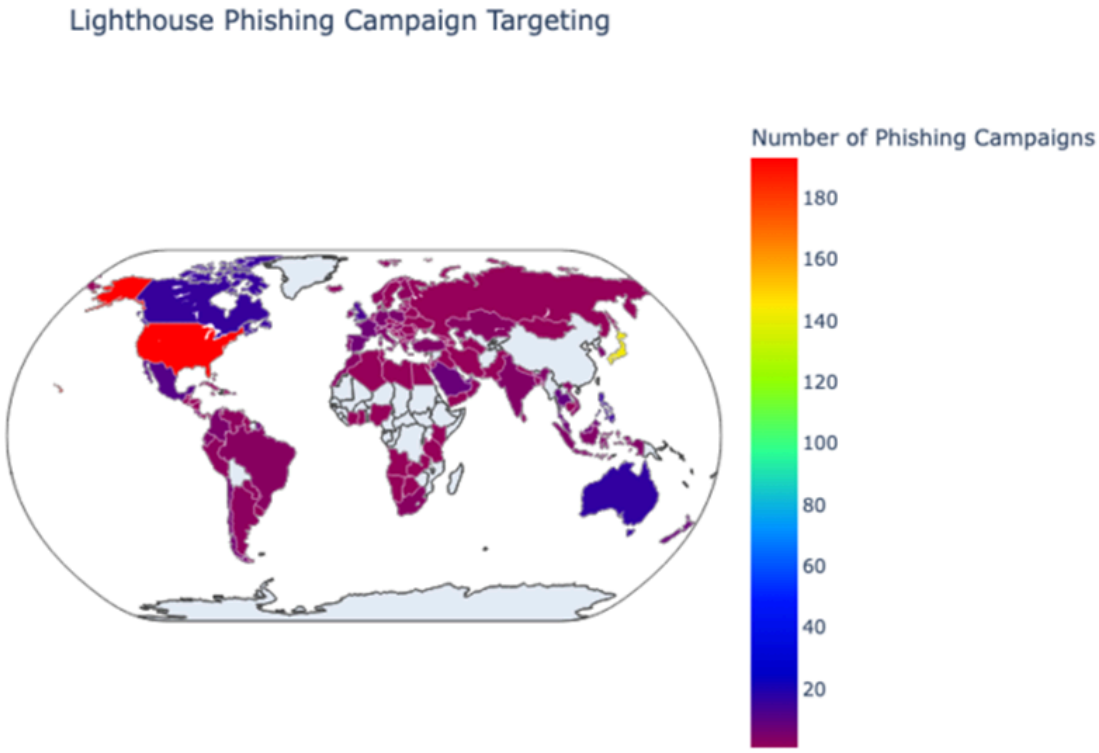
[10] Andreea Chebac, *What Is Phishing-as-a-Service (PhaaS) and How to Protect Against It*, HEIMDAL SEC. BLOG (July 7, 2025), https://tinyurl.com/ypjm4ae6.

[11] Lorenzo Franceschi-Bicchierai, *How the Mafia Is Pivoting to Cybercrime*, VICE (Sept. 22, 2021), https://tinyurl.com/2vym7aaa.



34. At least 197 templates target victims in the United States by mimicking the website of a U.S.-based institution. These templates included spoofed websites of toll collection agencies, financial institutions, shipping companies, retail companies, and even state and local governments. One spoofs the official website for New York City, as shown in paragraph 88 below. Other templates also spoof the West Virginia Department of Motor Vehicles, the Departments of Transportation for Virginia, Maryland, West Virginia, Wisconsin, Iowa, Michigan, and more.

35. The Lighthouse Scheme disproportionately targets U.S. victims, as demonstrated by the graphic below.



36. ***The E-Commerce Version.*** The e-commerce version of Lighthouse facilitates the creation of fraudulent e-commerce websites to steal victims' financial information. One version of this tool can be used to create a fraudulent website from scratch and integrate payment options that funnel user data to the Lighthouse software. These pages often spoof legitimate retail websites. The other version of the tool allows users to develop a fake storefront on a legitimate e-commerce platform.

37. Threat actors lure unsuspecting victims to the fraudulent e-commerce websites by advertising through various networks that distribute ads on internet and social media platforms.

38. ***Evading Detection.*** Both the SMS and e-commerce versions of the Lighthouse software have security features designed to help the fraudulent websites evade detection. For example, Lighthouse can notify users when a phishing domain has been flagged as suspicious. When this feature is activated, the Lighthouse platform automatically queries transparencyreport.google.com every fifteen minutes to determine whether Google has flagged a phishing domain as malicious. Similarly, Lighthouse markets a so-called anti-red feature, which is designed to notify the Enterprise when a fraudulent domain is flagged by web-browsers such as Chrome. If Chrome has identified a domain as malicious, Lighthouse's anti-red feature informs the Enterprise member who created the fraudulent website so he can change the website's domain to avoid detection.

39. ***Evading Two-Factor Authentication Security.*** Both versions of the Lighthouse software also allow threat actors to create fictitious multi-factor authentication ("MFA") pages, further deceiving targets into believing they are interacting with legitimate entities.

40. Many financial institutions implement MFA technologies to combat fraud, including by sending numerical codes via SMS or through a dedicated mobile application.

41. Lighthouse undermines MFA protections. Once a victim submits their payment information to either a fake e-commerce or SMS phishing website, the victim is directed to a fake MFA phishing page that prompts the victim to enter a code to verify the purchase.

42. While the victim waits to receive the code, the Enterprise uses Lighthouse to generate a visual representation of the victim's credit card.

43. The Enterprise then scans the Lighthouse-generated card image with a camera on a mobile device, and attempts to add the payment method to the device's digital wallet (such as Google Wallet).

44. Attempting to add the credit card as a payment method on a mobile device triggers the card's financial institution to send an actual MFA code to the victim.

45. The victim, believing that the code is being received in response to the victim's purchase authorization (and not realizing that it is in fact authorizing the fraudster to add a payment method to a mobile device) enters the code into the MFA phishing page.

46. The scammer receives the code through the Lighthouse software and inputs it on their mobile device, thereby completing the process of adding the victim's payment card to the digital wallet on the threat actor's mobile device. Once the victim's payment method is added to the mobile device, it can be used for fraudulent transactions without the need for additional MFA codes.

The Lighthouse Enterprise

47. The Lighthouse Enterprise includes several connected threat actor groups that design and implement complex criminal schemes targeting the general public. While different members of the Enterprise may play different roles in the Schemes, they all collaborate to execute phishing attacks that rely on the Lighthouse software. None of the Enterprise's Schemes can generate revenue without collaboration and cooperation among the members of the Enterprise. All of the threat actor groups are connected to one another through historical and current business ties, including through their use of Lighthouse and the online community supporting its use, which exists on both YouTube and Telegram channels, as described below. Although certain Enterprise members may serve multiple roles, the Enterprise is generally comprised of members who participate in the following groups:

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

49. It includes the individuals or entities that developed Lighthouse by designing and continuing to maintain and upgrade the system's software, architecture, and user interface, writing code to carry out its functions, and conducting testing. At least two individuals or entities have been attributed with developing or assisting with the development of the Lighthouse software; they are known by their online aliases "Wang Duo Yu" and "CoSmile."

50. The Developer Group creates templates to target new companies and victims, and it is responsible for providing ongoing maintenance and updates to Lighthouse.[12] Since March, it has issued 89 version updates that have upgraded the software's features, provided performance enhancements, fixed bugs, and made other adjustments to evade fraud detection efforts.

51. Anyone that purchases a license to use Lighthouse can connect with other members of the Enterprise who have the necessary expertise to execute the particular phishing scheme. These members include:

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

53. These individuals or entities supply targeted lists of potential victims' contact information to other members of the Lighthouse Enterprise, ensuring the Scheme reaches a wide number of targets in locations relevant to the particular phishing scheme.

54. The data brokers collect these bulk sets of contact information from a variety of sources, including public records, social media, and data breaches. Breached data is often sold on the dark web.

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

[12] For example, from August 6, 2025 to October 18, 2025, the Developer Group added 73 new templates, increasing the total number of available templates from 614 to 687.

56. Large-scale smishing schemes require infrastructure to facilitate sending mass text messages. To send thousands of text messages simultaneously, the Enterprise needs banks of smartphones, SIM cards, modems, and services to support the data that sending mass text messages demands. The Spammer Group provides these resources to other members of the Enterprise. For example, an individual, group of individuals, or entity acting under the username "@Gblockduoyu," referred to as "Kunlun," helps send the messages necessary to contact victims of SMS scams. Wang Duo Yu has referred to Kunlun as Lighthouse's "Official" RCS provider.

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

58. Once members of the Enterprise have acquired phished credentials from victims, the Theft Group uses the stolen information to access bank accounts, email accounts, brokerage accounts, and other sensitive accounts to make or steal money, obtain social security information, and acquire additional victim information.[13] Using Lighthouse's specific digital wallet functionality, the Theft Group can also load stolen payment cards to digital wallets like Google Wallet, and resell the card information or use it to make purchases. The Theft Group also helps to launder stolen money for the Enterprise's continued use.

59. For example, one member of this group goes by the alias "Seven," or @seven7zai. Seven helps other members of the Enterprise make cash withdrawals. Seven employs over 200 employees across Hong Kong, Taiwan, Malaysia, Vietnam, Japan, Thailand, and other European countries to assist the Enterprise.

[13] *See* Mnemonic Security Podcast, *The Economy for Phish* (Apple Podcast, Aug. 18, 2025), https://tinyurl.com/4dr3h52v.

60. Another member, "August," has helped other Enterprise members use credit card information or money obtained through the phishing scheme to purchase large quantities of tickets to global attractions, thereby laundering the proceeds of their crimes.

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

62. Part of the appeal of the Lighthouse software is the ease with which someone with limited technical expertise—like many members of the Enterprise—can purchase the software, learn how to create various phishing attacks, and, upon purchase, meet the other members of the Enterprise in online forums run by the Administrative Group.

63. The Administrative Group uses several Telegram and YouTube channels to facilitate the Enterprise's use of Lighthouse to carry out phishing attacks.

64. On YouTube, the Administrative Group runs a channel (which Google has suspended) that contains videos advertising Lighthouse. The videos instruct Enterprise members (and potential members) on how to use Lighthouse to carry out phishing attacks.

65. On Telegram, the Administrative Group operates several channels that are used for various functions. Through these channels, the Enterprise markets and sells Lighthouse, receives feedback from Enterprise members about the software and its functionality, connects Enterprise members to each other based on their specific specialties, and executes phishing and smishing schemes.

66. On one Telegram channel, members of the Enterprise can purchase licenses to use various versions of Lighthouse (either the SMS version or the two e-commerce versions). Originally, the Enterprise licensed the software through an online shop called "Lighthouse

Shop"; as of May 2025, Enterprise members can also order licenses through a "self-service ordering bot" available on the "@LighthouseShopBot" Telegram channel.

67. Members may subscribe to weekly, monthly, seasonal, annual, or permanent licenses.

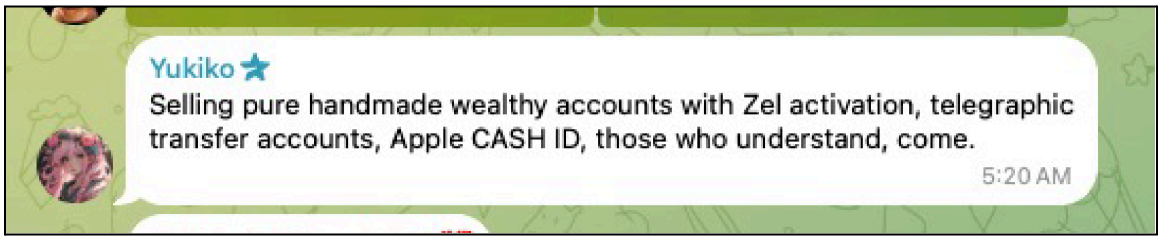
68. Another Telegram channel is a Lighthouse-related discussion group called the @laowangLiveGroup that includes over 2,500 members. There are seven administrators ("admins") of this channel, including @wangduoyu0 (a.k.a. Wang Duo Yu), @xiaobai77699 (a.k.a. Nutbrownbear), @zldfgrw (a.k.a. August), @seven7zai (a.k.a. Seven), @fyy8588 (a.k.a. CoSmile), @Gblockduouyu (a.k.a. Kunlun), and @cooler_chengz. Admins have authority to invite, ban, and remove members, and moderate content by deleting messages, "pinning" important messages, and controlling other chat settings.

69. These Telegram Channels are the primary locations where members of the Enterprise gather, discuss strategies and their respective areas of expertise, train each other, and develop and openly discuss specific Lighthouse phishing schemes.

70. Although these schemes are plainly criminal, the Enterprise brazenly coordinates their efforts on Telegram, including on the @laowangLiveGroup channel.

71. For example, on July 31, 2025, at 3:11 p.m., one user posted, "Who can send a few US live baits?" followed by two laughing emojis. Approximately 30 minutes later, another user asked, "Who is fishing? Looking for a partner." And within roughly an hour, two other users posted "[o]nline" in response.

72. On August 2, 2025, a user posted that they were selling account information: "selling pure handmade wealthy accounts with Zel[le] activation, telegraphic transfer accounts, Apple CASH ID, those who understand, come."



73. These Telegram groups coordinate with each other to recruit and train new members of the Enterprise, generate phishing strategies and tactics, select phishing targets, and coordinate phishing attacks. The Developer Group created the software and the Administrative Group markets it to recruit new members to the Enterprise. The Administrative Group also relays information about software updates to other members of the Enterprise, and relays information from Enterprise members about software issues back to the Developer Group. Through the Administrative Group's Telegram channels, members of the Enterprise can plan phishing attacks and connect with the Data Broker Group and Spammer Group to utilize those groups' expertise

and tools to execute attacks. Once the Enterprise has victim information in hand, the Theft Group sells or uses that information and helps to launder ill-gotten funds.

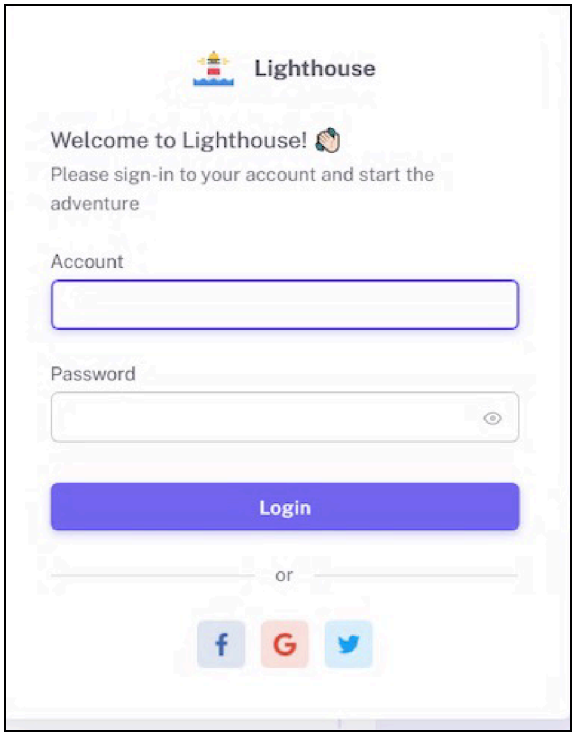
Fraudulent Schemes Perpetuated by the Lighthouse Enterprise

74. Four of the most well-known and commonly used SMS phishing schemes executed by the Lighthouse Enterprise are the Delivery Scheme, the Toll Scheme, the Financial Institutions Scheme, and the E-Commerce Scheme.

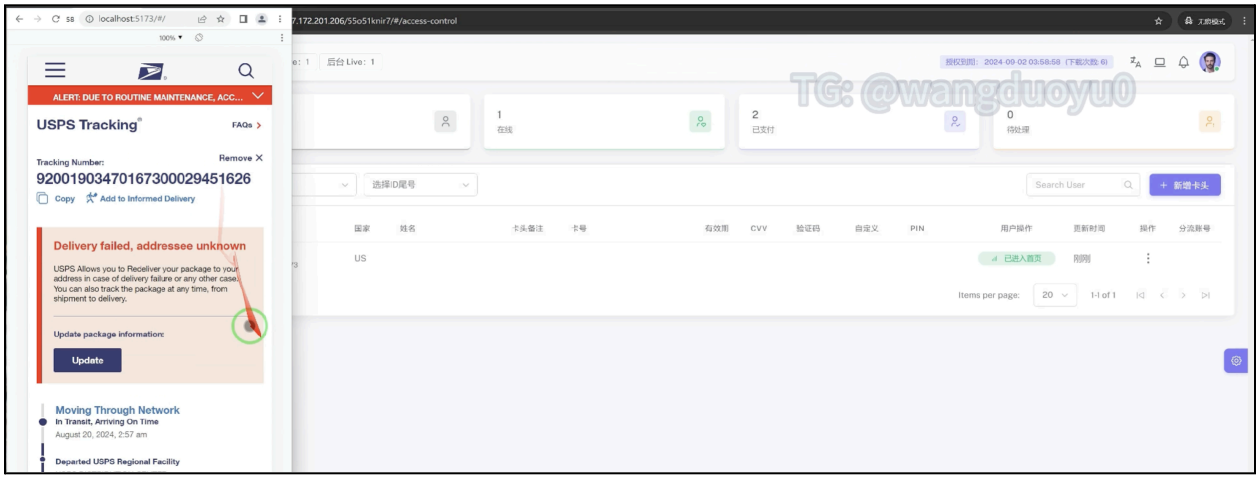
75. **Delivery Scheme.** The Lighthouse Enterprise's text-based spoof of USPS and other parcel delivery services is among the most prolific cyberattacks currently in operation. Researchers estimate that the Lighthouse Enterprise created and/or used 32,094 fraudulent unique USPS websites from July 2023 through October 2024, compromising anywhere between 12.7 million and 115 million credit cards in the United States alone.[14]

76. To execute a delivery scheme using Lighthouse, a member of the Enterprise simply logs in to a Lighthouse account through the portal shown below and determines which template he intends to use. Although the login page to the Lighthouse dashboard appears to allow the option to sign in with a Google account, the Google logo is not a functioning button.

[14] *See Research: The Evolution of Chinese Smishing Syndicates and Digital Wallet Fraud,* SecAlliance (Aug. 5, 2025), https://tinyurl.com/ym4wwxhd.



77. From there, Lighthouse generates a dashboard as depicted below.

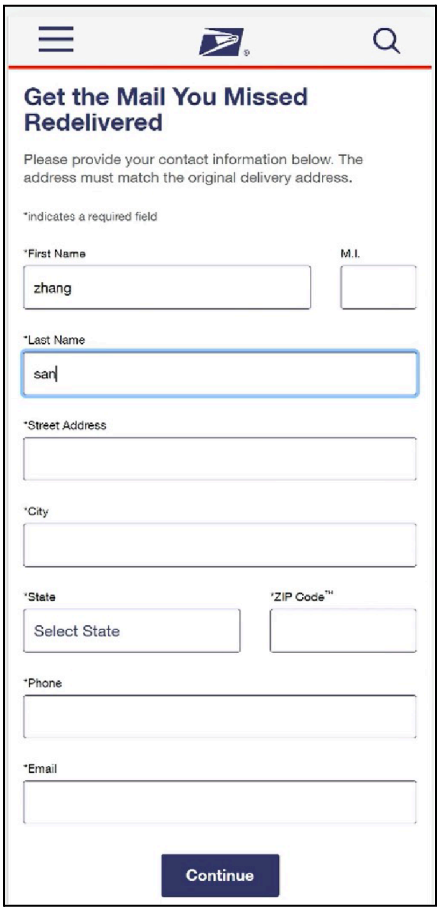


78. Those interested in executing this particular attack can connect with each other on the Lighthouse Telegram channels and work together to carry out the phishing attacks. For example, members of the Enterprise who do not have the technical capability to send out bulk texts can connect with the Spammer Group, which sends mass text messages for a fee.

79. The Enterprise member then sends the phishing texts to the targets, purporting to be, for example, USPS. Those texts inform targets that they have an undelivered package.

80. Targets are told that, to "complete delivery," they must pay a small delivery fee by clicking on the website link provided in the text message. That link directs the victim to a spoofed USPS website. Once on the website, individuals are prompted to enter personal identifying information.

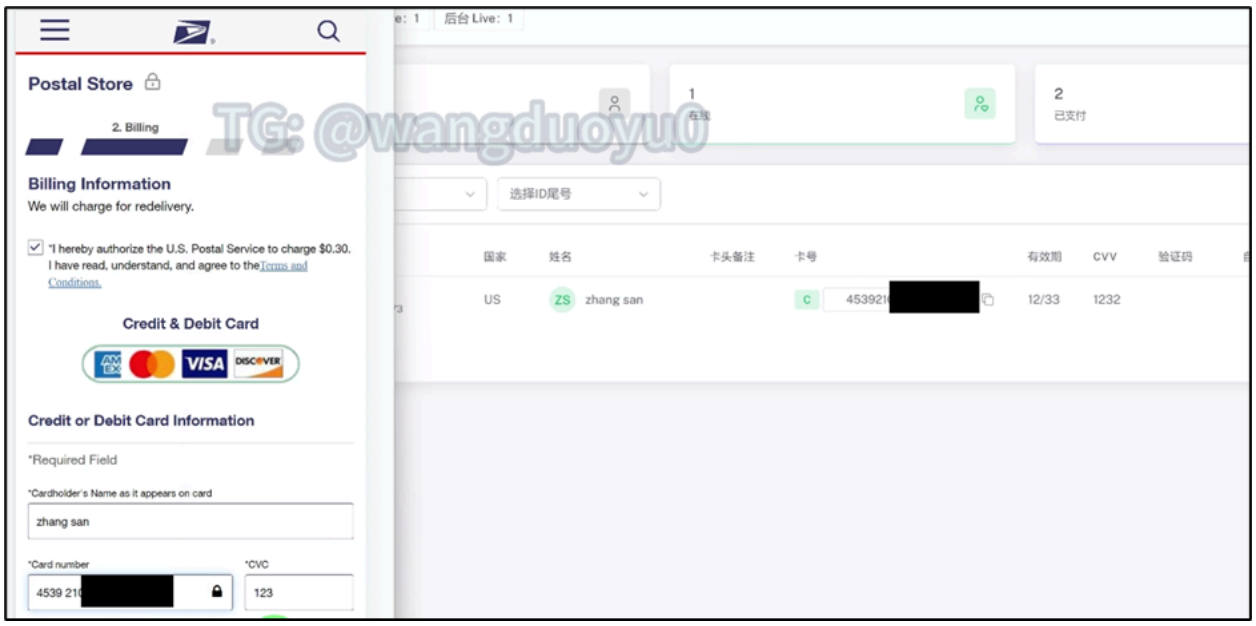
81. Believing the website to be genuine, targets input their address information into the form on the website, as shown below.



82. The fake website may say, for example, that USPS "will charge for redelivery." It may also include a check box saying, "I hereby authorize the U.S. Postal Service to charge $0.30. I have read, understand, and agree to the Terms and Conditions." As victims enter their personal

financial details, the Lighthouse interface simultaneously tracks their keystrokes. The victim thus need not actually submit the payment for the scammer to procure their payment information.

83. The Enterprise can then access that information by logging into their Lighthouse accounts. Because this feature collects and organizes victims' stolen data, it is easier for the Enterprise to use that stolen data.



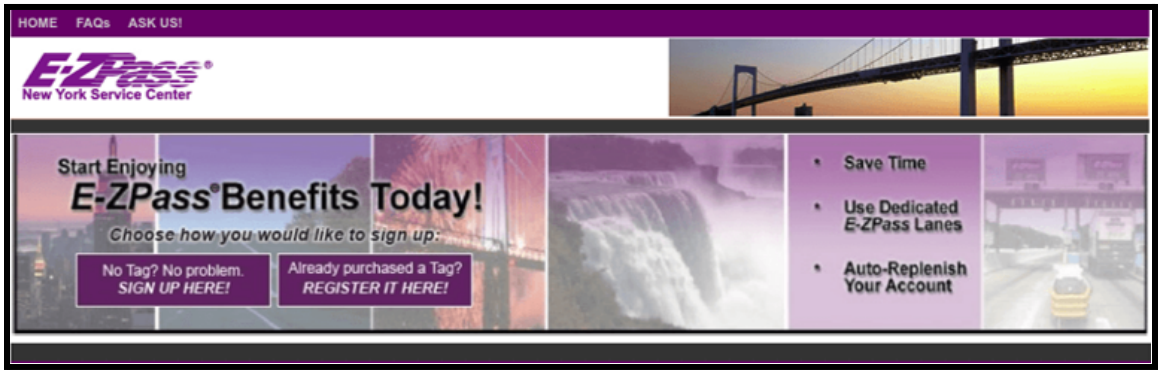
84. A member of the Enterprise using the username "@wangduoyu0" posted a tutorial on Telegram explaining how to use Lighthouse to perpetrate the USPS scam. The four-minute video describes how the scam works. The tutorial trains members of the Lighthouse Enterprise to use Lighthouse and deploy phishing attacks through their Lighthouse account.

85. **Toll Scheme.** Another scam commonly carried out by the Lighthouse Enterprise involves text messages concerning toll or ticket violations.

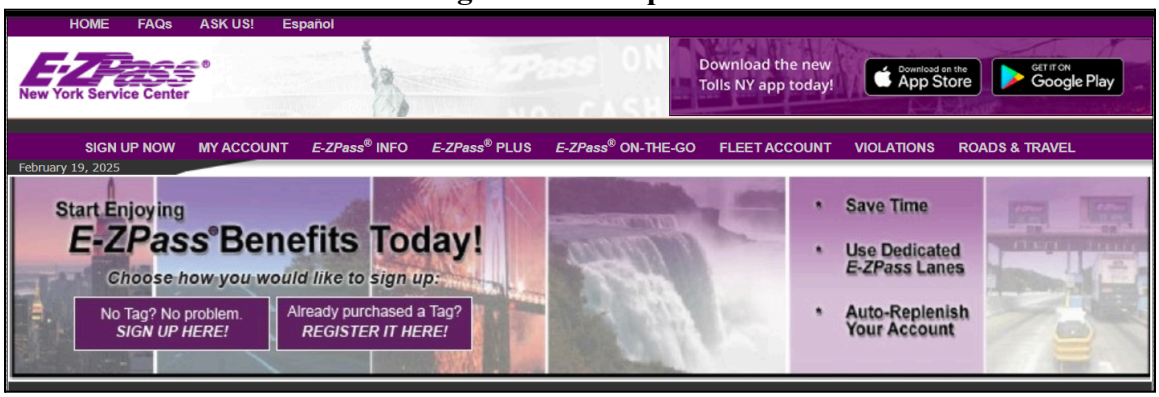
86. Lighthouse includes templates for 73 fraudulent toll collection websites and 19 fraudulent government websites that target victims in the United States. For example,

Lighthouse offers a fake version of the New York City government's website and a fake version of E-ZPass New York's website.

87. The Lighthouse websites are nearly indistinguishable from the legitimate websites they are designed to mimic. As shown below, for example, the Lighthouse version of the E-ZPass New York website is virtually identical to the real version.



Lighthouse Template[15]



Real Website[16]

88. The Lighthouse version of New York City's website (left, below) is also nearly identical to the legitimate version (right, below).

[15] This is a screenshot of Lighthouse's template for E-ZPass New York on or around February 19, 2025. Naxo Decl. Fig. 36.

[16] This is a screenshot of the E-ZPassny.com website as it appeared on or around February 19, 2025. WAYBACK MACH. INTERNET ARCHIVE, E-ZPass New York Service Center, https://tinyurl.com/23tasnt6.

Lighthouse Template[17]

Real Website[18]

89. Members of the Enterprise collaborate to execute the attacks. For example, the Data Broker Group can provide the Spammer Group with potential victims' phone numbers, and the Spammer Group in turn sends SMS or RCS messages in bulk to phone numbers, using geolocation information to match victims with appropriate local governments or toll collection agencies. The software enables users to customize the country they target using IP addresses' geolocations.

90. The targets then receive a text message purporting to provide notice of a past due toll invoice or ticket, along with a link to the fraudulent website. Like the delivery scam, the toll

[17] This is a screenshot of the Lighthouse phishing template for the NYC.Gov scam that was posted to Telegram on January 26, 2025. *See* Naxo Decl. Fig. 4.

[18] This is a screenshot of the NYC.Gov website as it appeared on or around January 25, 2025. *See The Official Website of the City of New York*, CITY OF N.Y., https://tinyurl.com/bz7scnru. The City has recently updated their website design.

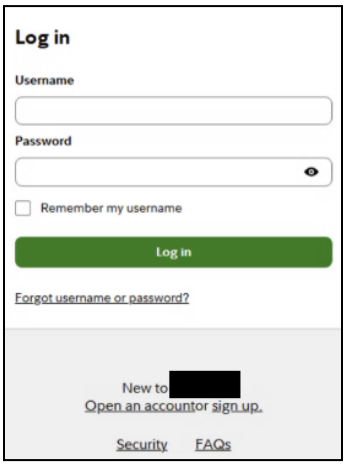
scam requests that targets input personal information, such as their credit card number and driver's license information, to pay the purported toll.

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

92. **Financial Institutions Scheme.** The Financial Institutions scheme functions similarly to the Delivery and Toll Schemes in that Enterprise members send text messages to unsuspecting users that contain links to malicious websites. In this scheme, however, the websites mimic those of reputable financial institutions, with the goal of gaining access to individuals' accounts. Enterprise members can select from a number of website templates that spoof popular financial institutions, including those that target consumers in the United States.

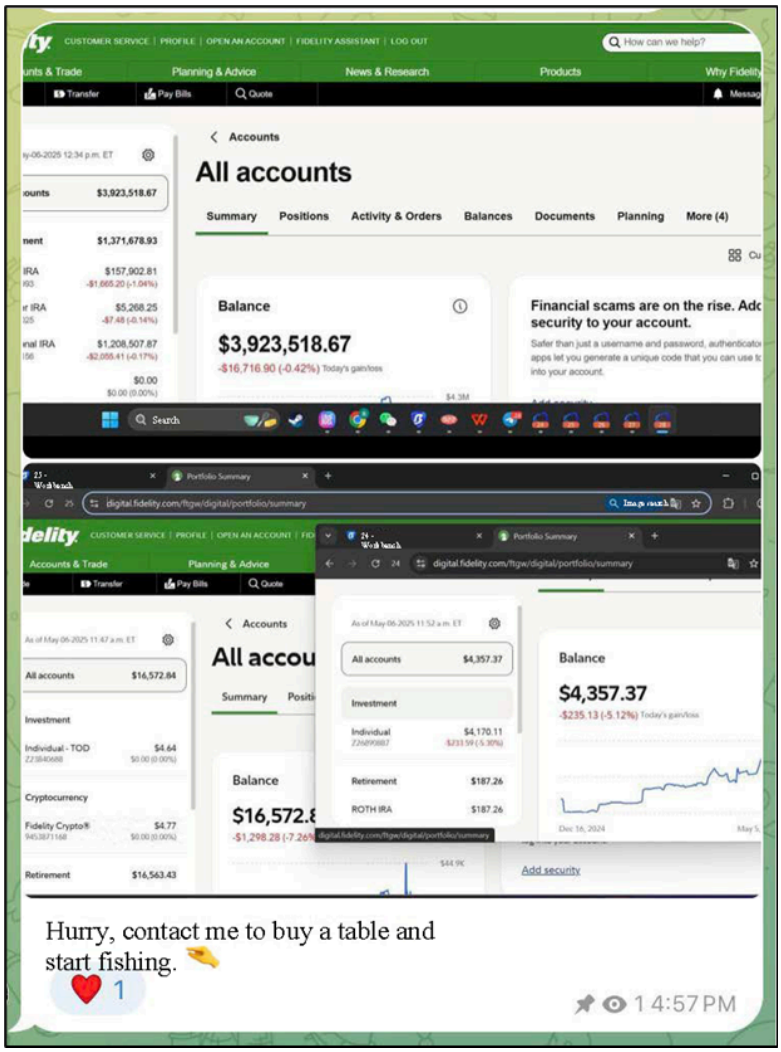
93. In one example, Enterprise members created a domain that mimics the website of a large, U.S. financial institution. The domain can only be accessed using a web browser on a mobile phone. Because mobile browsers typically have fewer security features, victims are less likely to be warned by a browser security feature designed to flag malicious domains.

94. When a target navigates to the domain, the user sees the below interface, which closely mimics the actual login page for clients with investment accounts at the financial institution:

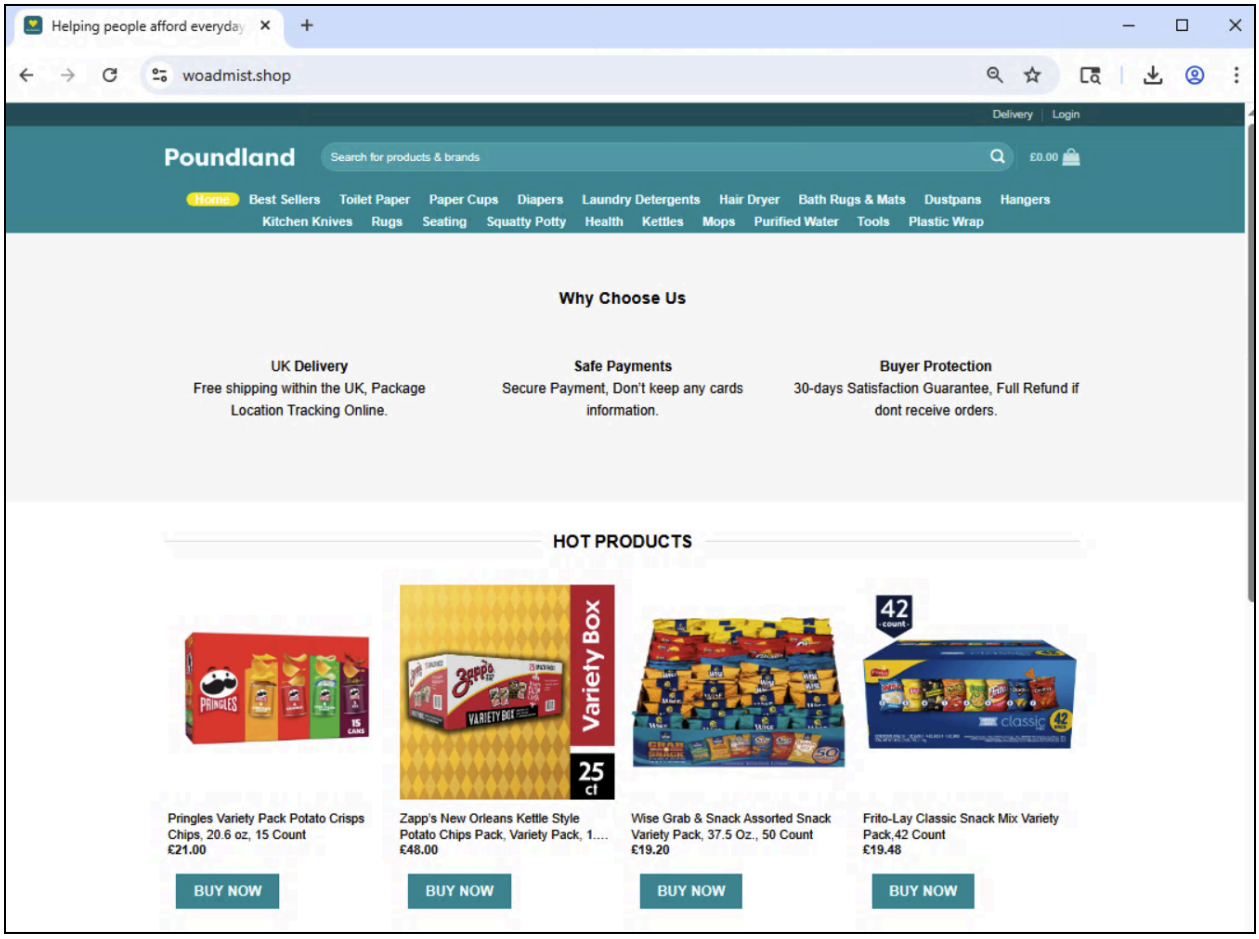


95. If the target enters their log-in information, Enterprise members who control the website will receive that information instantaneously on the Lighthouse dashboard, even if the target does not actually submit the information by clicking the "Log in" button. The Enterprise can then use those credentials to access the target's brokerage accounts and steal the funds.

96. The Administrative Group has used the prospect of access to brokerage accounts to encourage Enterprise members to purchase Lighthouse and conduct phishing attacks. For example, on May 6, 2025, @wangduoyu0 posted an image of an investment account with a balance of almost $4 million, along with the note, "Hurry, contact me to buy a table and start fishing." The "table" refers to Lighthouse, and "fish" refers to the victims of the fraud.



97. **E-Commerce Scheme.** The Enterprise also uses the e-commerce version of Lighthouse to defraud victims. Lighthouse enables the Enterprise to build fake e-commerce websites, like the below-pictured WoadMist[.]shop. The website displays a storefront with categories of different goods along with a heading that claims, "Safe Payments. Secure payment, Don't keep any cards information [sic]."



98. The website is then advertised on social media platforms, search engines, or other websites that support internet advertising.

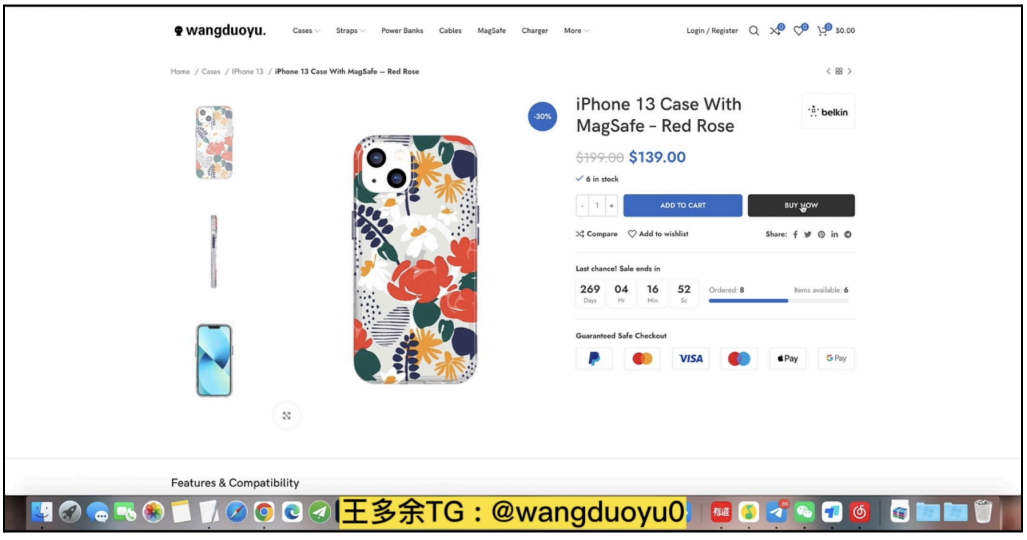
99. The Enterprise uses online advertising platforms—including Google Ads—to create ads that distribute links to their fraudulent e-commerce websites. Google has suspended the Enterprise's Google Ads accounts.

100. Members of the Enterprise create publisher accounts on these platforms by providing false contact information—including email addresses set up for criminal use and fake names—and stolen credit card information to pay for the accounts.

101. The Enterprise then uses their advertising accounts to publish online ads with links to fraudulent websites. Once the Enterprise deploys a phishing ad, the ad will become visible to targets browsing the internet, whether on social media accounts or other web browsers.

102. Once a target clicks on the advertisement, he or she is directed to the fake website. When the target attempts to complete a purchase, the website saves their financial information for members of the Enterprise to access and use. The website directs the victim to a landing page that indicates the purchase has been completed, often including a tracking or other confirmation number; however, the victim never receives the product because the shop does not exist.

103. The Enterprise can design the e-commerce website to offer a wide variety of products, ranging from groceries to reusable water bottles, and more. A tutorial video posted by the Enterprise shows an e-commerce website purporting to sell cell phone accessories, as shown below.



104. The phishing website featured in the tutorial includes text stating "Guaranteed Safe Checkout" followed by various logos of well-known, reputable electronic payment companies, including Google Pay. Indeed, when building a fake website, Lighthouse explicitly provides the option to include descriptions of the types of payments that are "accepted" by the website, including: "debit and credit card payments in 135+ currencies, as well as Apple Pay, Google Pay, Klarna, Affirm, P24, ACH, and more." This is a common feature of Lighthouse phishing websites and is specifically designed to give the target a sense of false comfort by spoofing reputable payment platforms. It also encourages users to enter Google Pay information that can then be stolen.

105. Below are several examples of this Scheme from just this year:

a. A Gmail account was created in 2010 and lay dormant until 2025. Accounts like these are known as "aged made-for-abuse" accounts, as the early creation date helps to make the account appear legitimate and avoid fraud detection efforts. A member of the Enterprise purchased the Gmail account and used it to sign up for a Google Ads account on August 2, 2025. From August 24, 2025 to September 11, 2025, the Google Ads account ran advertisements for a phishing domain created with Lighthouse software that is designed to mimic the website of a popular drinkware brand. During that period, targets clicked on the ads and were directed to the fake e-commerce store 217 times.

b. An Enterprise member purchased another aged, made-for-abuse Gmail account and used it to sign up for a Google Ads account on or about July 14, 2025. From August 4, 2025 to August 28, 2025, the Enterprise member used the Google Ads account to run ads for a phishing domain created with Lighthouse that mimics an

e-commerce shop selling beverage containers. During that period, targets clicked on the ads and were directed to the fake e-commerce store 1,020 times.

c. A member of the Enterprise purchased a third aged made-for-abuse Gmail account and used it to sign up for a Google Ads account on June 30, 2025. From August 2, 2025 to September 6, 2025, the Enterprise member used the Google Ads account to run ads for a phishing website created using Lighthouse that purports to sell a popular brand of stuffed animals. Over the month that ads were run through the registered account, targets clicked on the ads and were directed to the fake e-commerce store 1,062 times.

d. An Enterprise member purchased a fourth aged made-for-abuse Gmail account and used it to sign up for a Google Ads account on August 15, 2025. From August 15, 2025 to September 11, 2025, the Enterprise member used the Google Ads account to run ads for a phishing domain created using Lighthouse that mimics a popular supermarket chain. During that period, targets clicked on the ads and were directed to the fake e-commerce store 8,606 times. Google users reported the link as a scam, noting the website appeared designed to mimic the website of a popular supermarket chain.

106. The Enterprise has also used stolen credit cards to pay for its Google Ads accounts, uploading U.S.-issued credit cards that list either a Taiwanese or Chinese billing address, and foreign identification methods for identity verification. For example:

a. One account added a credit card for a U.S.-based banking institution on August 15, 2025. The billing address for this card is in China. Although the account holder made two payments using the card, other payment attempts were declined.

b. For another account, the holder added a U.S.-based credit card on August 16, 2025. The billing address for this card is in China. Although the account holder was able to make certain payments using the card, other attempts were declined.

c. Another holder added a U.S.-based credit card on August 12, 2025. The billing address for the card is in Taiwan. Although the account holder was able to make certain payments using the card, other attempts were declined.

d. Another holder added two U.S.-based credit cards on September 3, 2025, and another U.S.-based credit card on September 7, 2025. The billing address for both cards is in Taiwan.

107. The Enterprise has also used stolen identities in connection with account verifications. One billing account uploaded two methods of identification, each belonging to a different individual; another account uploaded a method of identification bearing a suspicious watermark, indicating that it is illegitimate or potentially stolen.

Harm to Google, its Users, and the Public

108. It is estimated that there have been well over a million victims of the Lighthouse Enterprise. One cybersecurity firm estimated that in a 20-day period, the Lighthouse Enterprise created roughly 200,000 fraudulent websites, with an average of 50,000 page visits per day.[19]

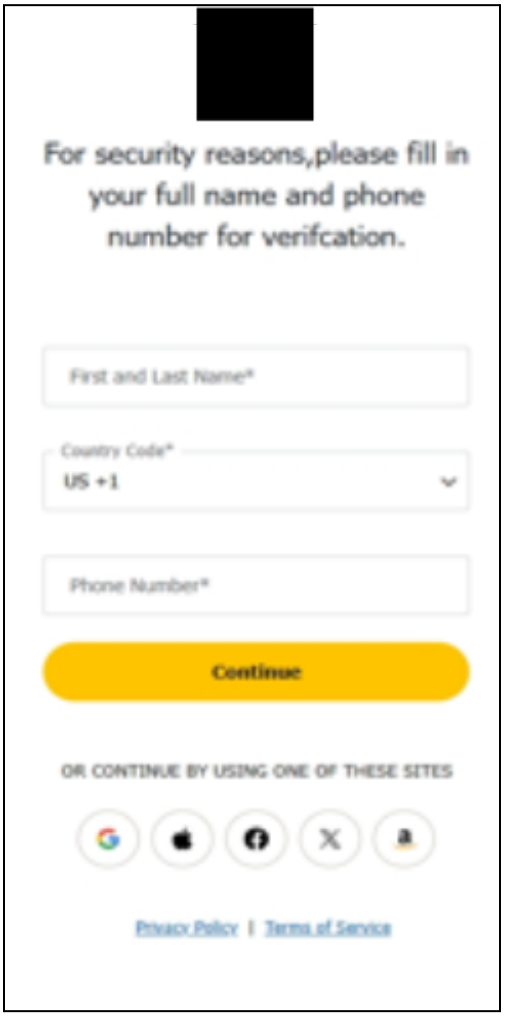
109. The Lighthouse Enterprise harms its victims by stealing their information, their money, and access to their accounts.

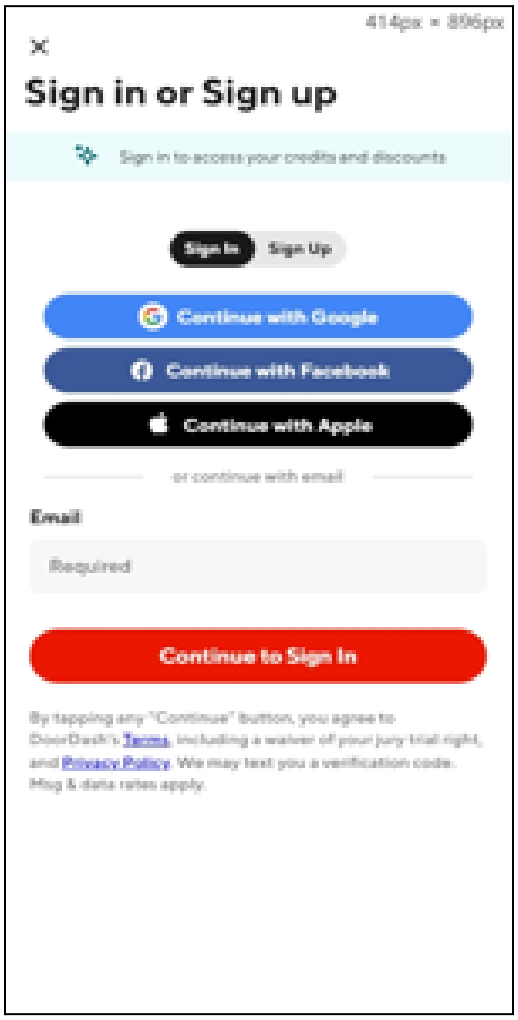
[19] *See Smishing Triad: Chinese eCrime Group Targets 121+ Countries, Intros New Banking Phishing Kit*, SILENT PUSH BLOG (Apr. 10, 2025), https://tinyurl.com/4m64c7pw. As noted above, *see supra* note 3, some security firms use the term "Smishing Triad" to refer broadly to Wang Duo Yu and other China-based phishing-as-a-service software developers, but Silent Push's research focused on the Lighthouse software.

110. The Lighthouse Enterprise harms Google by damaging customer trust and goodwill and forcing Google to invest significant time and resources in remediation efforts.

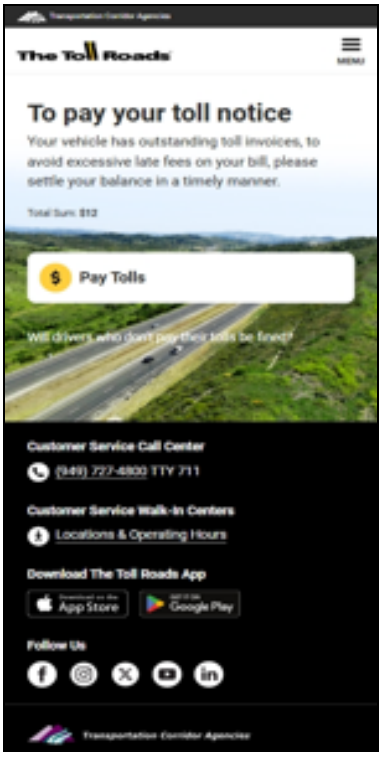
111. Specifically, the Enterprise has created and deployed at least 116 spoofed website templates featuring Google's branding or logos (YouTube, Gmail, Google, or Google Play) on the sign-in screen in an attempt to make the fake websites appear legitimate.

112. Some spoofed websites feature the Gmail logo, inviting targets to log in using their Gmail credentials.

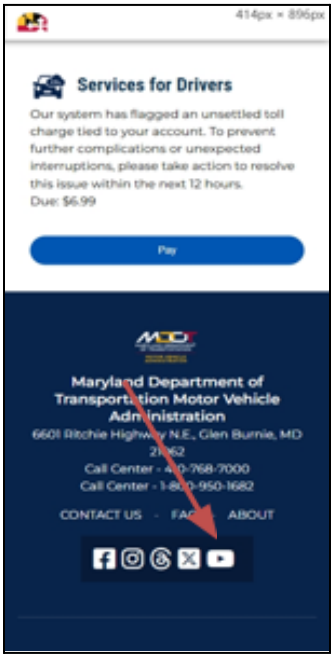


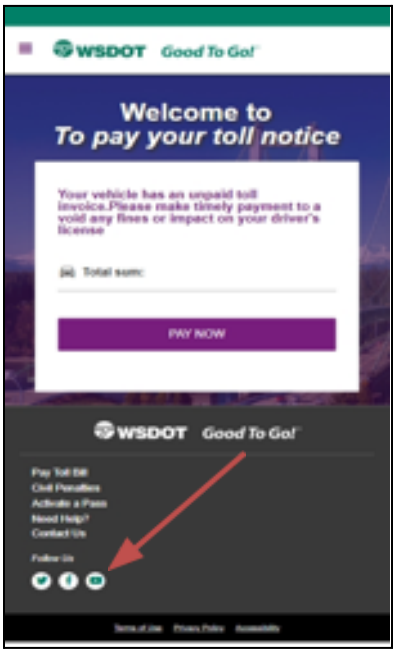


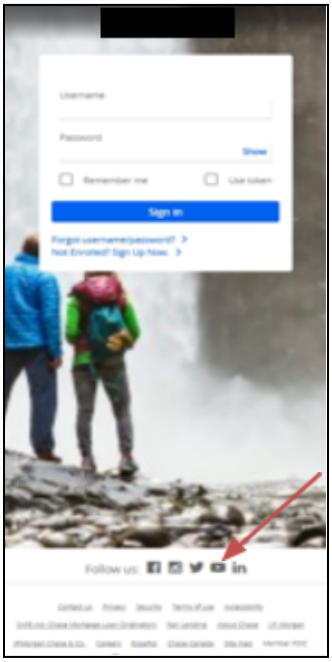
113. Other websites feature the Google Play logo, suggesting that targets can download the spoofed brand's app in the Google Play store.

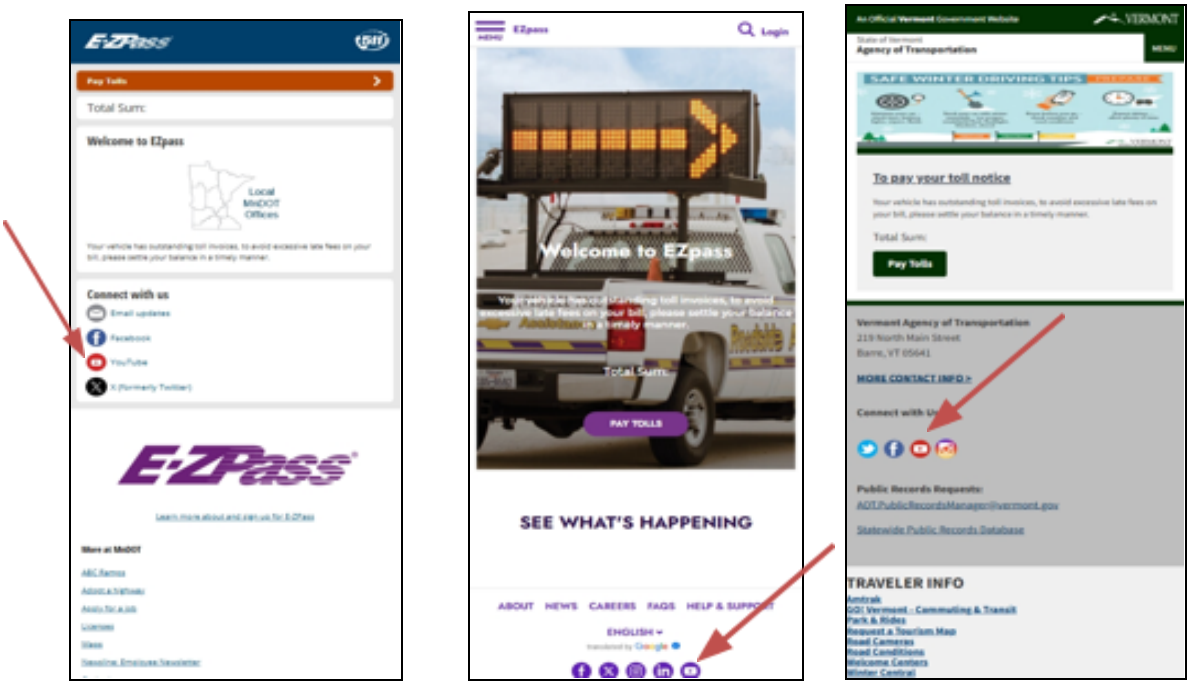


114. Other spoofed websites include the YouTube logo along with other prominent social media sites.









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

116. The Enterprise also used YouTube—a Google product—to recruit more individuals to the Enterprise by making instructional videos about using Lighthouse.

117. The exploitation of Google's product, branding, and logos harms Google's public image as a trustworthy company and may discourage customers from using Google's products and services.

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

Feature in a manner that is … misleading[] [or] infringing."[20] There are further requirements for the use of certain Google logos and icons. For example, Google's brand team must "review[] and fully approve[]" any use of the Google Play Mark.[21]

119. The Enterprise also uses Gmail accounts to create Google Ads accounts and publish advertisements to its phishing websites.

120. This use of Google products violates Google's Terms of Service, which requires account holders to agree that they will not be "accessing or using [Google] services in fraudulent or deceptive ways, such as … phishing" or "creating fake accounts."[22] The Enterprise facilitates illegal activities on Google's platforms and, therefore, causes damage to Google's customer relationships and reputation. Google actively investigates and terminates accounts supporting such activities as soon as possible.

121. To that end, Google has invested significant resources to combat the Lighthouse Enterprise and other cybersecurity threats. Google has spent hundreds of hours investigating and remediating Defendants' activities, including engaging investigations and product teams across four different countries, and suspending YouTube channels, Gmail accounts, and Google Ad accounts that supported the Enterprise's criminal activities. Google will continue these efforts.

CLAIMS FOR RELIEF

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

122. Google incorporates by reference the foregoing paragraphs (¶¶ 1–121) of the Complaint as if set forth in full.

---

[20] Google, *Rules for Proper Usage*, Brand Resource Ctr., https://tinyurl.com/24dvmced (last visited Sept. 15, 2025).
[21] Google, *Google Play Legal Requirements*, Partner Mktg. Hub, https://tinyurl.com/2yz2mscd (last visited Sept. 15, 2025).
[22] Google, *Terms of Service*, https://tinyurl.com/ynm67nz3 (last visited Sept. 28, 2025).

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

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

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

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

The RICO Enterprise

127. 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. Specifically, Defendants, as members of the Lighthouse Enterprise, have worked together over time to create, control, and use Lighthouse to execute numerous criminal schemes that harm and threaten to continue to harm Google, its users, and the general public.

128. As described *supra* at paragraphs 47 through 107, Defendants have organized themselves into a network of cybercriminals operating in the United States and overseas, targeting victims in the United States. Over time, they have adapted their operations and schemes, enlisted new threat actors, and expanded the scope and range of their activities.

129. Utilizing Lighthouse to execute a wide variety of phishing schemes, Defendants act with the common purpose of enriching themselves by fraudulently obtaining sensitive personal and financial information. Specifically, Defendants have collaborated to establish, grow, and manage the Lighthouse Enterprise and its Scheme, and deploy the Lighthouse software. Members of the Enterprise take part in directing aspects of the Scheme: some develop the Lighthouse software; others manage the Telegram and YouTube channels where Lighthouse

is marketed and sold; others supply lists of targets' contact information; still others provide strategies for sending out bulk SMS messages; others help steal money and social security information with phished credentials; and still others help launder the money.

130. Defendants constitute an association-in-fact enterprise within the meaning of 18 U.S.C. §§ 1961(4) and 1962(c). The existence of this association-in-fact enterprise is evidenced by Defendants' membership and communications in the Lighthouse Telegram channels, common use of Lighthouse, coordination in executing specific phishing attacks, and the commercialization of the attacks, which indicate that Defendants function like a black-market business enterprise. *Supra* ¶¶ 47-73.

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

Pattern of Racketeering Activity and RICO Predicate Acts

132. At all relevant times, Defendants conducted or participated, directly or indirectly, in the conduct, management, or operation of the Lighthouse Scheme 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.

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

134. Google was injured in its business and property by reason of the Defendants' violations of 18 U.S.C. § 1962(c), as described herein, including through Defendants' phishing

schemes and by having to devote substantial financial resources to combat Defendants' criminal activity. These injuries are a direct, proximate, and reasonably foreseeable result of these violations, and Google will continue to be harmed absent the relief requested here.

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

135. 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.

136. The Defendants commit wire fraud in violation of 18 U.S.C. § 1343 each time that they:

a. Use online advertising platforms to distribute links to websites falsely purporting to be legitimate e-commerce sites designed to trick the owner of a device into submitting sensitive personal or financial information;

b. Create Gmail accounts and Google Ads accounts using fake names and stolen credit card information to deploy fake ads impersonating legitimate brands; and

c. Send text messages containing links to websites falsely purporting to be government agencies, financial institutions, and other legitimate brands to trick the target into unknowingly disclosing sensitive personal or financial information, as detailed in paragraphs 74 through 96.

137. Google has suffered injury to its business or property as a result of each of these wire fraud predicate offenses, including the substantial investments it has made to investigate and disrupt these acts and its payments to the Enterprise for ads that deliberately promote websites intended to defraud those who navigate to the websites.

Conspiracy to Violate RICO

138. Google incorporates the foregoing paragraphs (¶¶ 1–141) of the Complaint as if set forth in full.

139. 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).

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

141. Defendants agree to direct or participate in, directly or indirectly, the conduct, management, or operation of the Lighthouse Enterprise through a pattern of racketeering activity in violation of 18 U.S.C. § 1962(c). Each Defendant knew about and agreed to facilitate the Lighthouse Enterprise's affairs. The purpose of the conspiracy was to commit a pattern of racketeering activity in the conduct of the affairs of the Lighthouse Scheme, including the acts of racketeering set forth above and the sale and use of Lighthouse to commit crimes, all for the purpose of enriching the Enterprise.

142. 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.

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

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

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

145. Google incorporates the foregoing paragraphs (¶¶ 1–148) of the Complaint as if set forth in full.

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

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

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

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

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

150. Defendants' and/or their agents' use of Google's Marks has caused and/or is likely to continue to cause confusion with Google's federally registered Marks, in violation of 15 U.S.C. § 1114(1). The use by Defendants and/or their agents of the Marks has caused and/or is likely to continue to cause confusion and mistake, has deceived and/or is likely to continue to deceive potential customers and the relevant purchasing public as to the source, origin, or sponsorship of Defendants' services, and has deceived and/or is likely to continue to deceive the

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

151. Google has no adequate remedy at law, and, if Defendants' actions are not enjoined, Google will continue to suffer irreparable harm to its reputation and the goodwill of its well-known Marks.

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

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

153. Defendants' and/or their agents' use of the Google Marks 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 the Google Marks and/or images associated with Google has caused and/or is likely to cause confusion and mistake, has deceived and/or is likely to continue to deceive potential customers and the relevant purchasing public as to the source, origin, or sponsorship of Defendants' services, and has deceived and/or is likely to continue to deceive the public into believing that those services originate from, are associated with, or are otherwise authorized by Google, to the damage and detriment of Google's reputation, goodwill, and sales.

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

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

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

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

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

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

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

160. 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.

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

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

163. 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.

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

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

165. Google incorporates the foregoing paragraphs (¶¶ 1–176) of the Complaint as if set forth in full.

166. Defendants have violated and continue to violate the CFAA, including 18 U.S.C. § 1030(a)(6), resulting in loss as defined in 18 U.S.C. § 1030(e)(11) to one or more persons during a one-year period amounting in the aggregate to at least $5,000 in value.

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

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

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

170. Defendants' conduct affects interstate and/or foreign communications.

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

172. Specifically, Google has suffered loss in the form of reasonable costs of responding to Defendants' scheme, including conducting damage assessments. *See* 18 U.S.C. § 1030(e)(11). Over the period from January 2025 to present, those losses have exceeded $5,000.00.

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

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

PRAYER FOR RELIEF

WHEREFORE, Google prays for judgment as set forth below:

A. Judgment in favor of Google and against Defendants;

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

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

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

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

F. Judgment awarding Google actual and/or statutory damages from Defendants adequate to compensate Google for Defendants' activity complained of herein and

for any injury complained of herein, including but not limited to interest and costs, in an amount to be proven at trial;

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

H. Judgment awarding attorneys' fees and costs; and

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

Dated: November 12, 2025

Respectfully submitted,

DRAFT

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

Christine M. Carletta
KING & SPALDING LLP
1700 Pennsylvania Ave., N.W., Suite 900
Washington, DC 20006-4707
Tel: (202) 737-0500
Fax: (202) 626-3737
ccarletta@kslaw.com

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

Counsel for Plaintiff Google LLC