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 Does 1–25 (the "Defendants") for injunctive relief and damages. Google alleges as follows:

INTRODUCTION

1. Defendants are a group of foreign-based cybercriminals who have made sophisticated fraud as simple as a few clicks of the mouse. They built, maintain, and use a turn-key, online software suite that enables criminals, regardless of technical skill, to publish fraudulent websites designed to rob victims and enrich themselves. With this "phishing-for-dummies" software—called "Outsider"—fraud that previously required technical sophistication is readily accessible. And the threat is only growing with the use of artificial intelligence ("AI"). In late 2025, phishing attacks generated using AI reportedly increased more than fourteenfold and now account for over half of all reported phishing incidents.[1] Google is suing to disrupt this criminal enterprise and to protect its users and the online ecosystem they use every day.

2. As with prior phishing scams, the fraud typically starts with a text message. But where prior scams lured victims with messages alerting them to missed packages or overdue highway tolls, these latest scams attempt to dupe victims by alerting them to a purported problem with their brokerage account, or insisting they are eligible for rewards through their mobile phone carrier. The text then links to a website that mimics the purported source of the text—for example, the investment manager or phone carrier—and then dupes victims into disclosing personal and financial information. Of course, the website is a fake, and the information goes to the scammers, who exploit it for their own criminal gain.

[1] Eliot Baker & Maxime Cartier, *Phishing Trends Report 2026*, Hoxhunt (2026), https://tinyurl.com/3c485zwv.

3. This type of scam is called a phishing attack. The key to the phishing attacks at issue in this action is Outsider, the powerful phishing software created by Defendants. For a subscription fee as low as $88 a week, the Outsider "phish kit" allows its users to create fraudulent websites, launch phishing campaigns, and steal victims' credit card numbers, bank account credentials, and personal data. The criminal enterprise in this case (the "Outsider Enterprise" or "Enterprise") includes the creators and administrators of this kit, as well as the criminals who license and use it to perpetrate these scams.

4. Like other phish kits, Outsider offers more than 290 pre-built templates that mimic the legitimate websites of trusted institutions—from financial services providers that maintain brokerage accounts, to wireless telephone service providers, government agencies, and retailers. It also provides real-time keystroke logging, and even a sleek performance dashboard to track the success of a criminal's phishing campaign—all from a single interface. The Enterprise also created and maintains an online community of discussion forums where members of the criminal Enterprise can identify other members with necessary skillsets (such as mass-texting or harvesting incoming financial information) and collaborate to execute a particular attack.

5. As a result, a criminal with no programming knowledge can, for example, generate a near-perfect replica of a cellular provider's website in minutes, coordinate to send "bait" text messages to thousands of targets, and begin harvesting stolen data with little effort. Indeed, the Outsider software has been used to create over a million phishing websites to swindle innocent victims out of millions of dollars.

6. As if Outsider's plug-and-play simplicity were not alarming enough, the Enterprise has made the tool even more powerful by providing step-by-step instructions on how Outsider can weaponize AI-generated code. Following those instructions, Enterprise members can use AI tools

to generate programming code for a shell website, and copy and paste that code into Outsider to transform that shell into a fraudulent site that can be used to steal personal or financial information from their victims. This means that the more than 290 website templates represent only a starting point—the number of distinct phishing sites that the Enterprise can create is effectively limitless.

7. Google has implemented multiple safeguards to ensure that Gemini is used responsibly, safely, and legally. Gemini imposes content filters that block certain categories of dangerous content, and it maintains security systems designed to detect malicious use, including the creation of malware and other cybercrime. When Google identifies users attempting to exploit Gemini, it investigates and disables offending accounts, and uses its findings to strengthen Gemini's safety systems. These efforts are central to Google's commitment to protecting its users and its products. This litigation is part of those efforts.

8. Google has also developed Safe Browsing, a security feature of the Google Chrome web browser that displays warnings to users when they attempt to navigate to sites that Google has identified as malicious or compromised. Users take these warnings seriously: when Google configured Safe Browsing to include and display warnings on Outsider-related phishing sites, traffic to those sites dropped dramatically.

9. The Enterprise exploits Google's reputation for safety and security in numerous ways. It features Google trademarks (the "Marks") on its fraudulent websites to lend a false veneer of legitimacy to its criminal schemes. The Enterprise abuses Google Cloud infrastructure by using it to host phishing websites, and at one point, linking to Google Drive to store stolen data. Google has devoted hundreds of hours and significant financial resources to investigating and remediating these harms.

10. The scale of the Outsider phishing attacks is astonishing. In the five-month period from November 14, 2025, to April 14, 2026, alone, Google detected more than 1.59 million URLs[2] linked to the Outsider Enterprise. This number is not static—on the one hand, Google and other companies work to thwart phishing attacks, and, on the other, the Enterprise launches thousands of new sites every day. But the sheer volume of URLs created in a mere five months reflects the Enterprise's massive scale and productivity. And its criminal efforts are effective: an earlier version of the software was responsible for the theft of at least 36,000 payment cards issued from financial institutions in 95 countries.

11. Google brings this action under the Racketeer Influenced and Corrupt Organizations Act ("RICO") and the Lanham Act to disrupt this illicit activity, to prevent the Enterprise from causing further harm, and to recover damages.

PARTIES

Plaintiff

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

13. Google is a leading technology company that offers a variety of services in support of its mission "to organi[z]e the world's information and make it universally accessible and useful."[3] Its search engine, accessible at www.google.com, is the most widely used internet search service in the world.

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

[2] A URL (or "uniform resource locator") is a web address: a string of text that defines the specific location of a site, image, or document on the internet (*e.g.*, www.google.com).
[3] Google, *Our approach to Search*, https://tinyurl.com/27uasm7h (last visited June 10, 2026).

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

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

c. **Gemini**: Gemini is a family of AI models and tools. The Gemini chatbot (hereinafter "Gemini") allows users to submit requests using plain-language prompts to generate text, images, or even computer code.

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

e. **Google Drive**: Google Drive is a cloud-based storage service primarily designed for personal use.

f. **Google Cloud**: Google Cloud is a scalable cloud-based service primarily designed for businesses and developers to store and manage large amounts of data.

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

h. **Google Play**: Google Play is Google's 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 countries worldwide.

i. **Google Safe Browsing**: Google Safe Browsing is a security feature that helps protect over five billion devices every day by showing warnings to users when they attempt to navigate to dangerous sites or download dangerous files. Safe Browsing also notifies webmasters when their websites are compromised by malicious actors and helps them diagnose and resolve the problem so that their visitors stay safer. Safe Browsing protections work across Google products and power safer browsing experiences across the internet.

j. **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.

k. **Rich Communication Services ("RCS")**: RCS is a transmission protocol that lets users send messages and share files, including high-resolution photos, over mobile data and Wi-Fi. Messages sent via RCS use Google's RCS infrastructure. RCS chats between Google Messages users are end-to-end encrypted by default to keep users' conversations secure.

l. **YouTube**: YouTube is an online video-sharing platform.

15. Google strives to provide its users worldwide with safe and secure platforms. Google invests substantial resources to monitor, identify, understand, and ultimately disrupt a range of cybersecurity threats around the world—including harmful phishing operations like the one run by the Outsider Enterprise.

Defendants

16. 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 Outsider Schemes 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.

17. 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 Outsider Enterprise.

18. Google is presently aware of several connected Doe scammer groups within the Outsider Enterprise. It is not clear how many individuals compose each group nor how many groups compose the Outsider Enterprise; the Doe numbers are meant to be representative. These scammer groups use overlapping infrastructure and interact to support and develop the Enterprise's criminal schemes. The groups and their misconduct are described in more detail below.

JURISDICTION AND VENUE

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

20. 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.

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

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

23. 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 ("PhaaS")

24. As personal devices and email have replaced telephone lines and traditional mail, criminal activity has evolved and is leveraging those media 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 phishing schemes have grown dramatically. Cybercriminals are sending an estimated 3.4 billion phishing emails every day.[4] Phishing has become the most ubiquitous form of criminal fraud.

25. Phishing is a type of cyberattack in which scammers trick individuals into disclosing sensitive information like passwords, credit card numbers, or banking information, often by impersonating well-known brands, government agencies, or even people the victims know. The attacker typically targets individuals with emails, text messages, or 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 scammers then steal for criminal use.

26. Short Message Service ("SMS") phishing scams (or "smishing") refer to phishing attempts conducted by text message or other telephone messaging services like RCS and iMessage (as opposed to email). These messages, which can target thousands of phone numbers at a time, encourage recipients to click a link that appears to take victims to the entity being impersonated (*e.g.*, the bank, toll agency, or mail carrier) but in fact leads to a fraudulent phishing website maintained by the scammer.

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

27. 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 webpages are often fake stores on legitimate retail websites. Customers may inadvertently wind up on these websites when shopping on a retail website, or scammers can direct customers to these websites through internet advertisements.

28. Once scammers have victims' financial information in hand, they can use it to steal from the victims (and enrich themselves) in various ways. 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."[5] Some recent law enforcement actions have identified criminal networks that use phones loaded with stolen credit card information and tap-to-pay functionality to purchase gift cards in bulk.[6] Other groups simply purchase their own tap-to-pay machines and then use stolen victim cards to make payments directly to themselves.[7]

29. Still others use stolen brokerage firm credentials to perpetrate a modern form of a "pump and dump" scheme. The criminals begin by purchasing their own shares of a particular stock and then use compromised brokerage accounts to purchase large volumes of the stock in the

[5] Insikt Grp., *Ghost-Tapping and the Chinese Cybercriminal Retail Fraud Ecosystem*, Recorded Future: Cyber Threat Analysis (Aug. 14, 2025), https://tinyurl.com/3z9sa9jk.
[6] 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.
[7] *See* Brian Krebs, *How Phished Data Turns into Apple & Google Wallets*, KrebsOnSecurity (Feb. 18, 2025), https://tinyurl.com/32arezcj.

victims' names. After the victims' purchases drive the stock price up, the scammers exit their original positions.[8]

30. These schemes have proven to be so profitable that markets have formed to develop and sell tools necessary to execute these scams to would-be perpetrators. Indeed, PhaaS providers are known to compete with, and even steal from, one another. The result is that these criminals often build security and undetectability into their software to guard not only against detection by authorities but also to stave off this black-market analogue of intellectual property theft.

31. 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 and execute a phishing campaign. The software, sometimes referred to as a "phish kit" or "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. The automation and ease that phishing kits provide make these attacks less resource-intensive and ultimately more frequent.

32. The PhaaS model also makes it difficult to stop phishing attacks. As one cybersecurity firm has observed, "[c]atching 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."[9]

[8] *See* Brian Krebs, *Mobile Phishers Target Brokerage Accounts in 'Ramp and Dump' Cashout Scheme*, KrebsOnSecurity (Aug. 15, 2025), https://tinyurl.com/532xpfwf.
[9] Andreea Chebac, *What Is Phishing-as-a-Service (PhaaS) and How to Protect Against It*, Heimdal Sec. Blog (July 7, 2025), https://shorturl.at/2BgbX.

33. 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."[10] Mafia organizations also use phishing schemes to support their offline criminal conduct.[11]

The Outsider Software

34. Members of the Enterprise market the Outsider software as a new and improved system that allows scammers to create and execute phishing schemes with minimal effort.

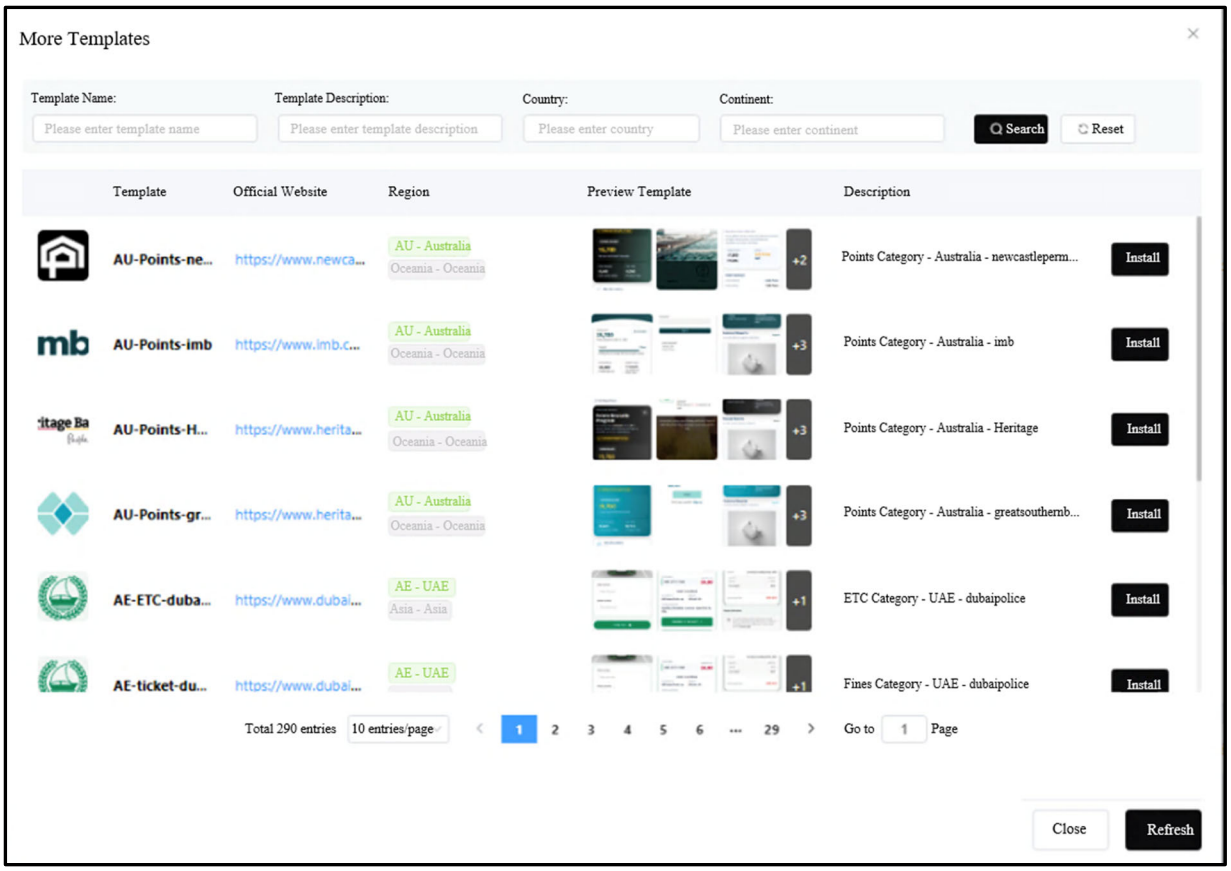
35. Using Outsider, Enterprise members can create phishing websites using either templates the software provides or templates the user designs themselves.

36. **Outsider Phishing Templates.** Outsider contains more than 290 website templates scammers can choose from. Each template is designed to mimic the legitimate website of a real entity or institution in order to dupe victims into providing their financial information and other personal details.

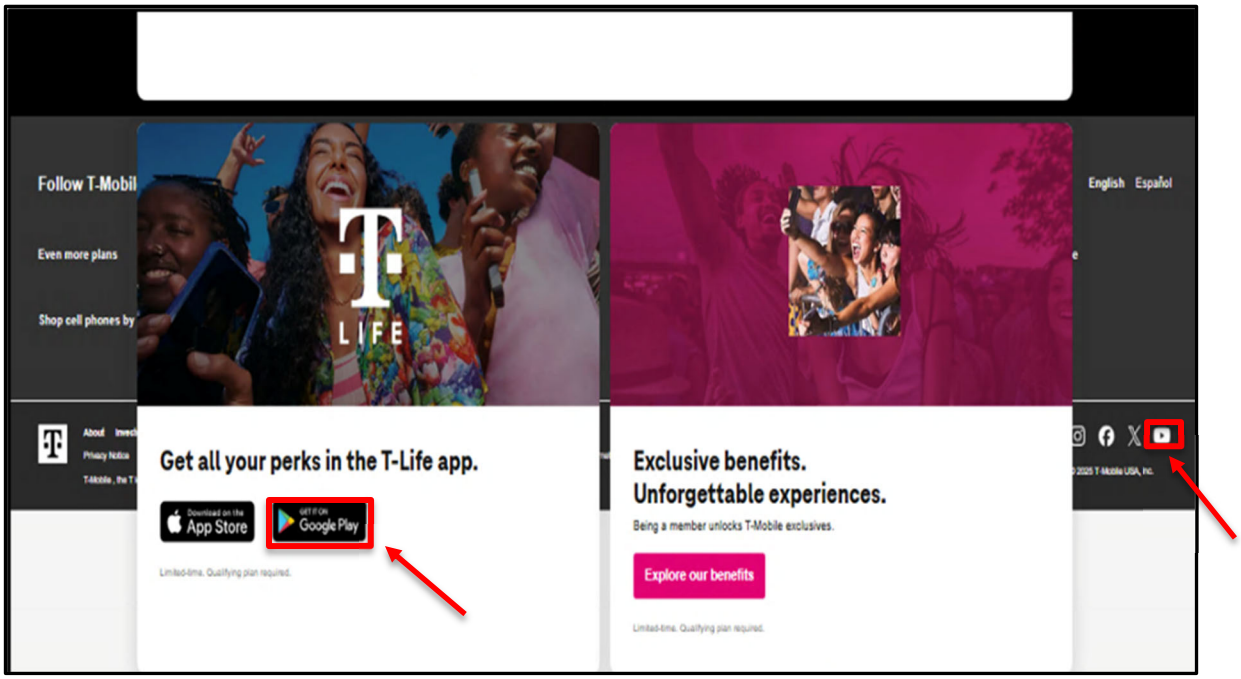
37. From the Outsider dashboard, Enterprise members can access a menu of available templates (pictured below), which they can filter for geographic region, country, or even the domain name of the site they intend to mimic. Once they select a template, they can customize it with various features and deploy it nearly instantaneously.

[10] *How the Mexican Drug Cartels Relate to Cybersecurity*, DefendEdge (Feb. 3, 2025), https://tinyurl.com/5y98hdkp; *see also Fueling Cartels' Cybercrime*, The Cyber Edge (Oct. 1, 2025), https://tinyurl.com/mu9pc7yh.

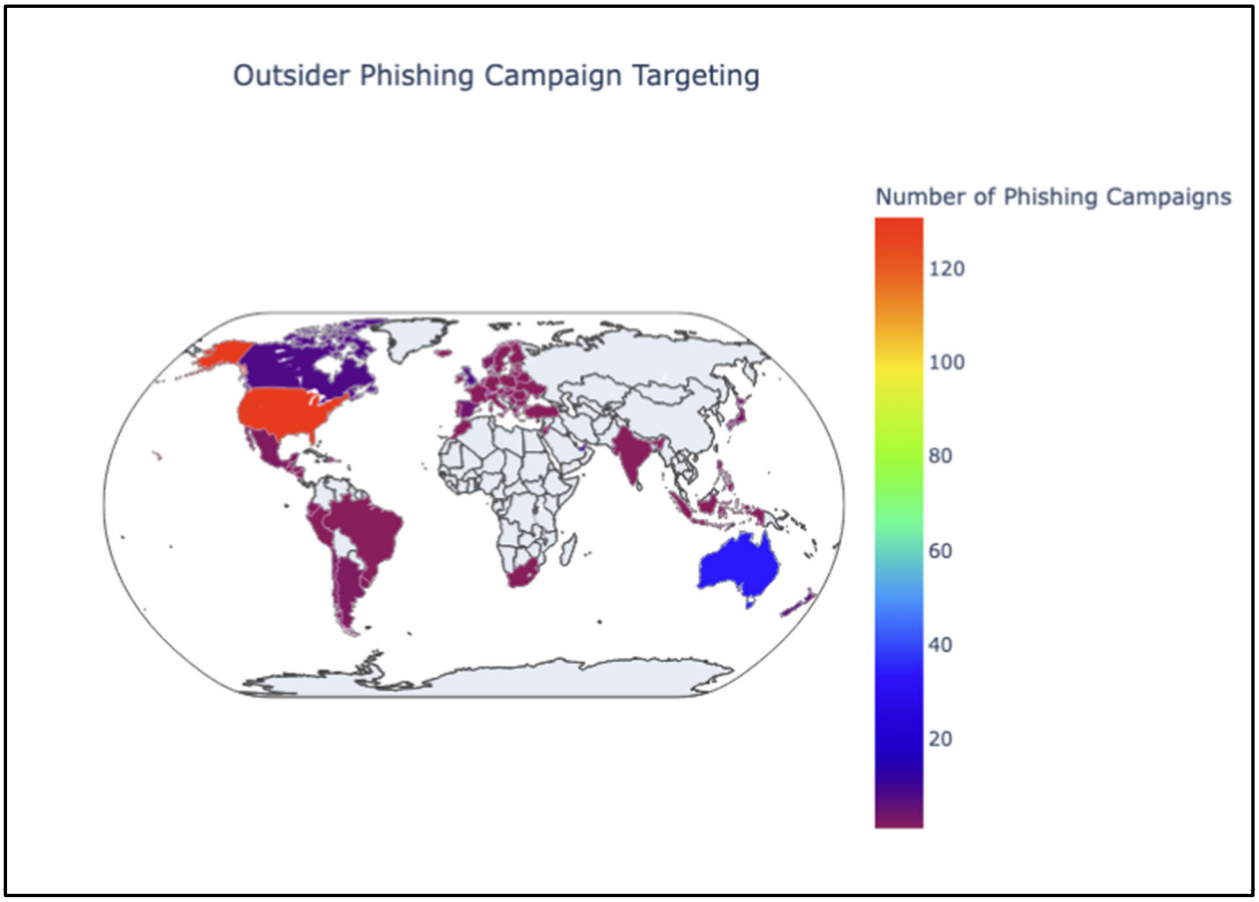
[11] Lorenzo Franceschi-Bicchierai, *How the Mafia Is Pivoting to Cybercrime*, Vice (Sept. 22, 2021), https://tinyurl.com/2vym7aaa.



38. At least 14 Outsider-provided templates feature a Google logo, including YouTube, Google Pay, and Google Play, as pictured below.



39. At least 131 templates target U.S. victims by mimicking the websites of U.S.-based institutions. More templates target the U.S. than any other single country, as demonstrated in the graphic below. These templates include spoofed websites of telecommunications companies, toll-collection agencies, brokerage firms, shipping companies, e-commerce sites, and even state and local governments. One template mimics the website for New York City, and another mimics New York E-ZPass, the widely used toll and payment service, as shown in paragraph 124 below. Others replicate the District of Columbia Department of Motor Vehicles, the Los Angeles Department of Transportation Parking Violations Bureau, and the United States Postal Service.

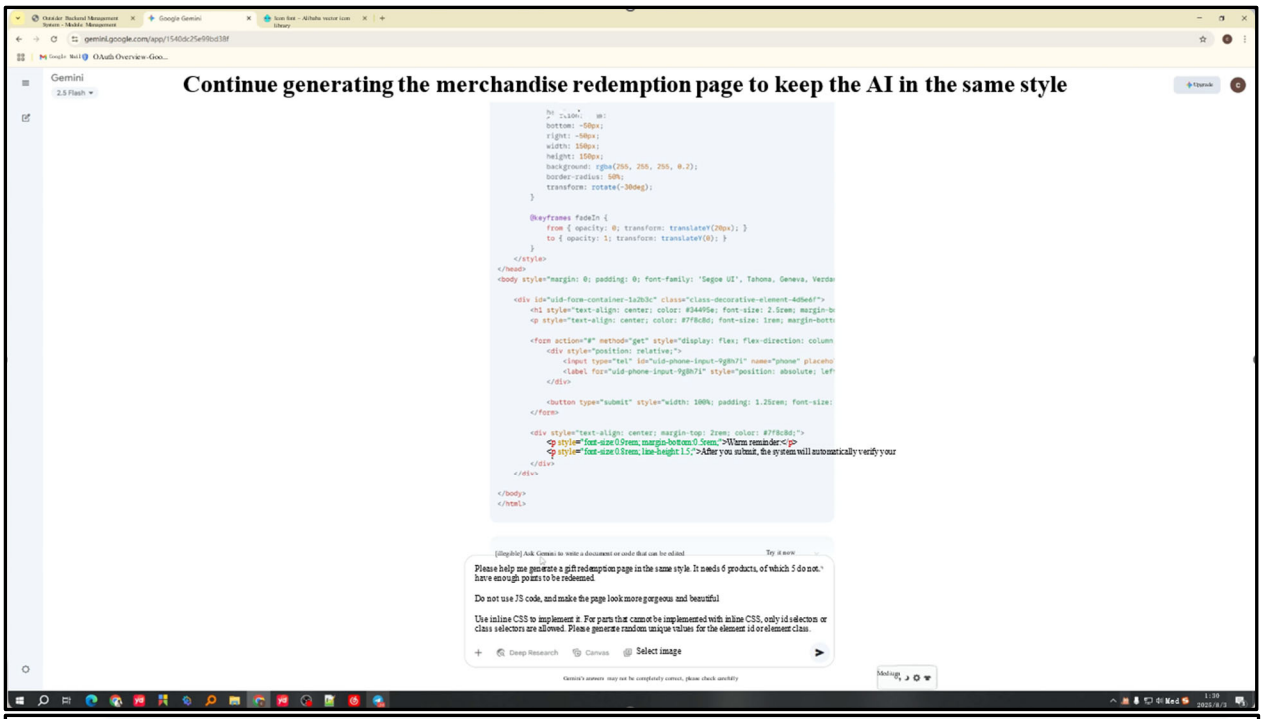


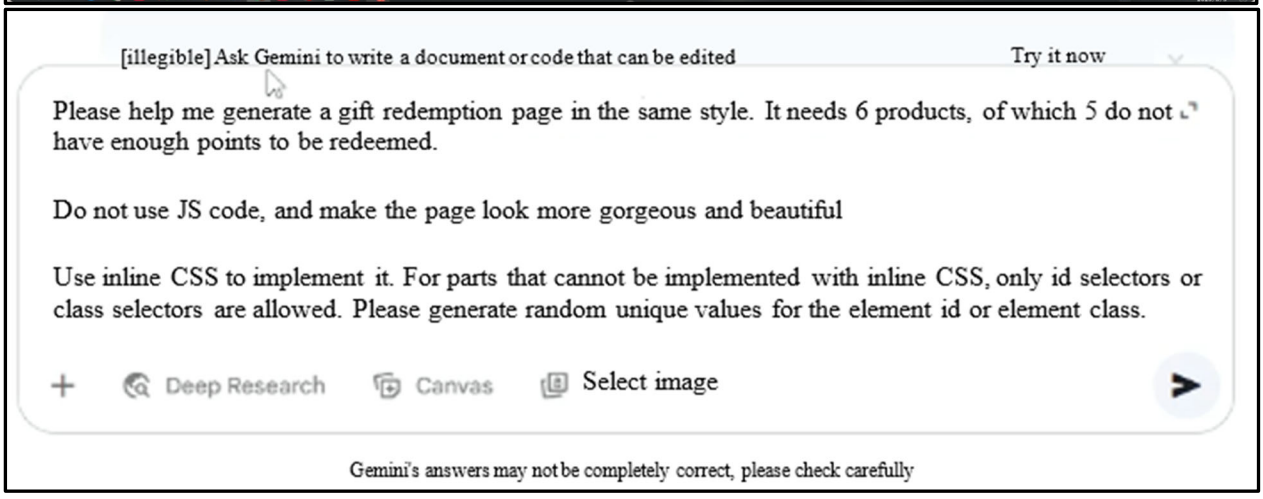
40. **Outsider's Use of AI.** The Outsider software also allows scammers to create their own websites by entering custom HTML code into the software platform. That functionality allows scammers to code a custom page that serves as a shell to which Outsider can add features that

facilitate criminal phishing activity. The Enterprise encourages scammers to use AI platforms, such as Google's Gemini, to write the custom code necessary to create their shell websites. On their own, these prompts appear to be innocent requests for programming assistance. Scammers, however, paste the AI-generated website shell code into Outsider to turn it into a phishing website that can, for example, funnel victim keystrokes straight to the Enterprise. Using this method, Enterprise members can create convincing duplicates of virtually any legitimate website in minutes. This means the actual number of unique phishing sites that Enterprise members can create is effectively unlimited.

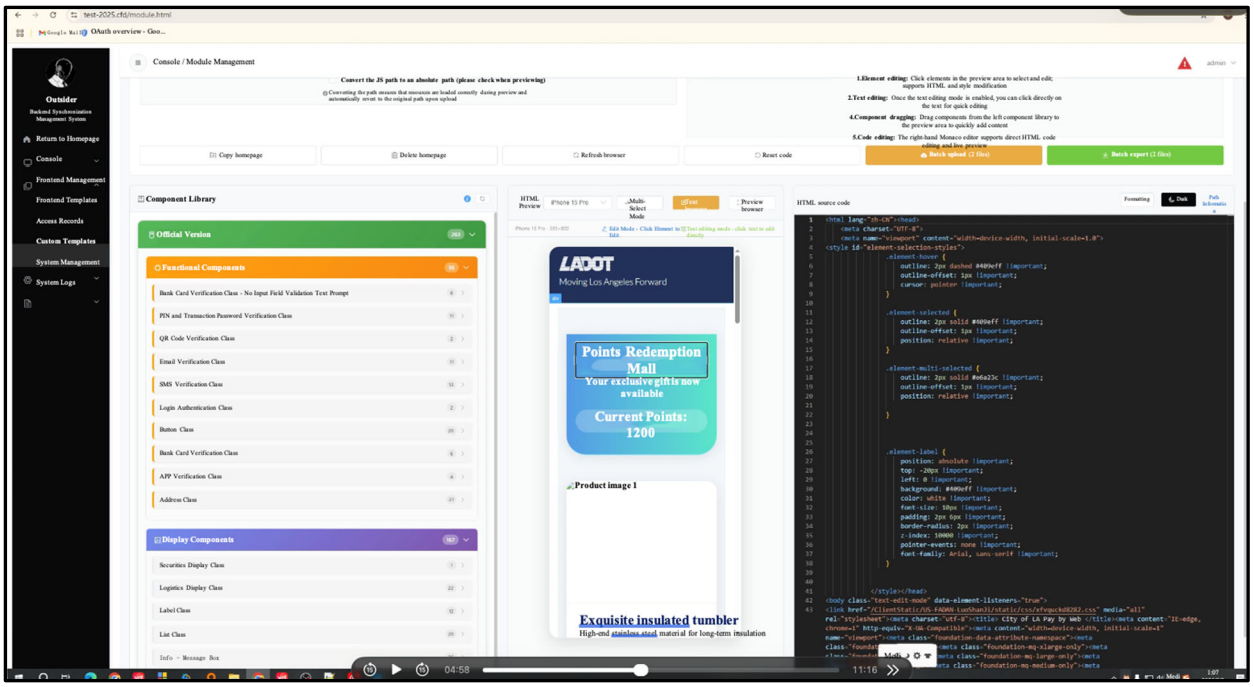
41. The Enterprise has made generating website code easy by releasing a tutorial video with step-by-step instructions on how to use Gemini. Other tutorial videos provide similar instructions for other AI platforms.

42. To start, scammers simply ask Gemini to generate software code in a programming language (usually, HTML) that can design a website with the desired functionality and features. The image below of the Enterprise's tutorial video shows this step, in which the Outsider user asks Gemini to design a "gift redemption page."



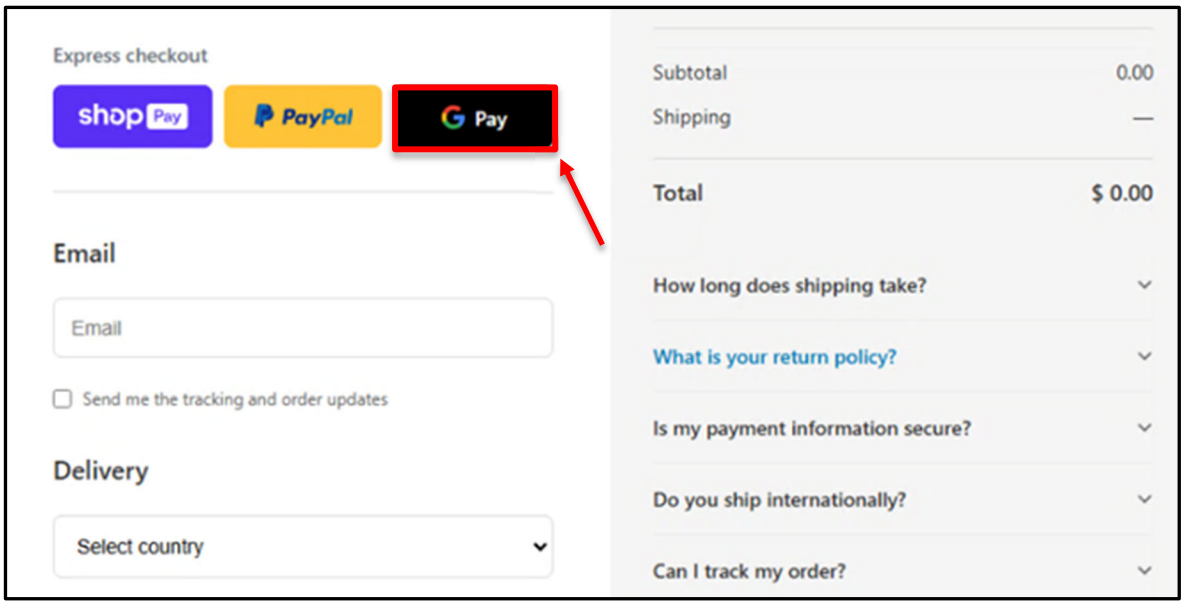


43. Once Gemini has generated the code, the Enterprise member then copies Gemini's code output and pastes it into Outsider's "custom template" editor, allowing the user to further customize the page, such as by inserting saved images of products or logos. Outsider then renders a preview of the fraudulent site—no computer-programming skills required.



44. Google has implemented multiple safeguards to ensure that its AI products are used responsibly, safely, and legally. Among those safeguards are content filters designed to prevent Gemini from producing certain types of content and security systems to detect malicious uses of the tool, such as the creation of malware or other cybercriminal activity. When this activity is detected, Google investigates and takes corrective action—including disabling offending accounts—and uses its findings to strengthen Gemini's safety systems.

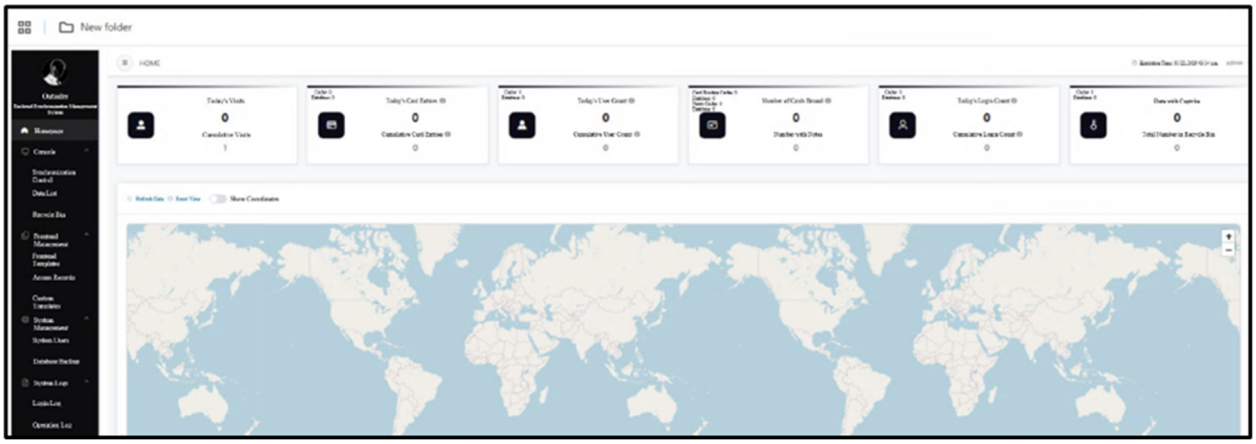
45. The scammer can also use Outsider's customization tools to add logos for Google Pay, Google Play, and/or YouTube to the phishing site, as shown in the images below. By adding these images, the spoofed websites can include the same logos and features present on real websites, thereby enhancing their perceived legitimacy.



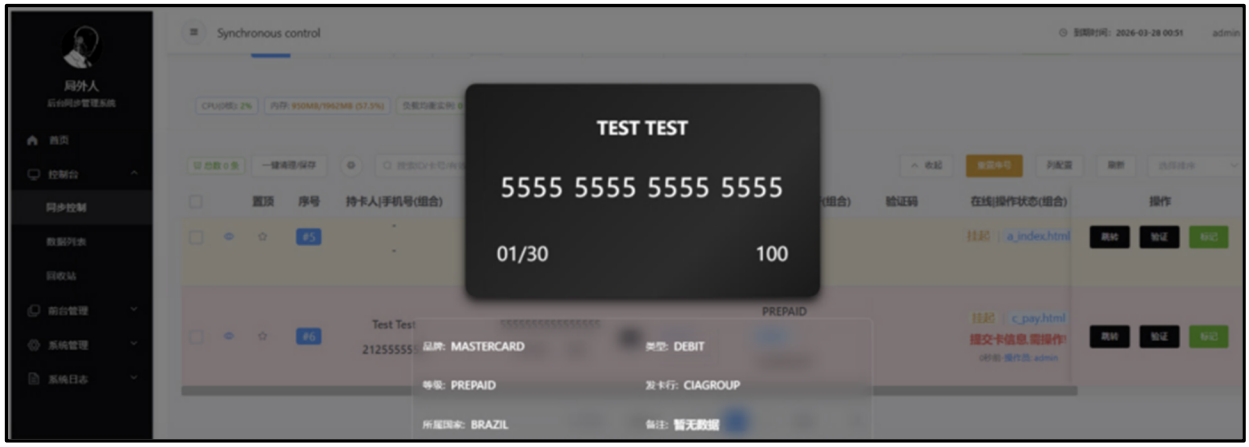
46. **Monitoring Attacks.** Once a phishing site is online, the Enterprise member can coordinate with other Enterprise associates to send the website's URL to potential victims by text message, often called "bait" messages. The Enterprise deploys these "bait" messages in text messages sent via Apple iMessage, RCS, and SMS. Not all scammers have the tools necessary to send bait messages in bulk. As outlined further below, the Enterprise hosts messaging forums on the encrypted Telegram application[12] where members can locate one another to collaborate, plan, and execute attacks.

47. Once messages are sent, Enterprise members can track their results on their Outsider homepage. As shown in the figure below, the Outsider homepage contains a unique dashboard for each user displaying real-time metrics on the phishing attacks. Using this dashboard, the scammer can easily monitor how many people visited the site and provided login or credit card information.

[12] Telegram is a free, encrypted messaging service with more than one billion monthly active users who communicate through channels and chat groups. Telegram channels are designed for one-way information sharing, where channel administrators can post in the channel to share information with channel members.



48. Outsider also provides the perpetrator immediate access to the data a victim divulges. The software tracks the victim's keystrokes and relays that information to the Enterprise member in real time. As the victim types their information, Outsider automatically formats the captured digits to resemble a standard credit card number, as shown below.



49. By generating images that resemble physical cards, the software enables the scammers to load stolen credit card data onto mobile wallets for use with tap-to-pay systems.

50. **Evading Two-Factor Authentication Security.** The Outsider software also allows scammers to create fictitious multi-factor authentication ("MFA") pages on phishing websites, further deceiving targets into believing they are interacting with legitimate entities.

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

common form of MFA is 3-D secure, a security protocol used by major credit card networks under brand names such as Visa Secure, Mastercard Identity Check, and Google Secure Payment Authentication. MFA requires a user to prove not only that they *know* something unique to them (*e.g.*, a password), but also that they *have* something unique to them (*e.g.*, their mobile phone or authenticating app).

52. The Outsider software undermines MFA protections by issuing its own fraudulent request for MFA and then using the victim-supplied information to log into the real site. When a victim enters their payment or login information to either a fake e-commerce or SMS phishing website, the Enterprise takes that information and begins to log into the real site (for example, adding the user's credit card as a payment method on a mobile device) using the victim's information. This triggers the real site to request an authentication code available only to the victim.

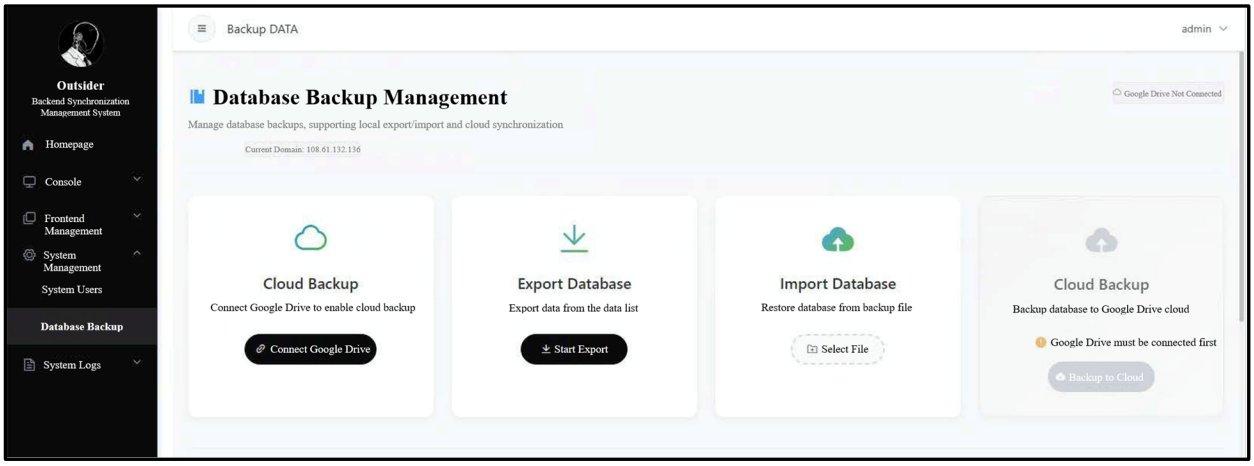
53. At the same time, the Enterprise responds to the victim—from the fake site—by asking for an MFA code. This causes the victim to look to their device for the code necessary to log into the institution being impersonated. And, because the Enterprise has indeed caused that institution to issue a code, a code is ready for use. 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 fraudulent MFA phishing page.

54. The scammer thus receives the code from the victim through the Outsider software, which they can then use to complete the process of adding the victim's payment information to the digital wallet on the scammer's own 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.

55. The Outsider software allows scammers to request multiple types of verification from victims, including SMS, PIN, email, and app verification. This flexibility enables the Enterprise to defeat various forms of authentication security, including 3-D secure protections that would otherwise prevent unauthorized credit card transactions.

56. **Google Drive Storage.** To support the scale of the Enterprise's operations, the Outsider software integrated a "database backup" function to store stolen data. That feature integrated Google Drive's cloud storage functionality. With a few clicks, Enterprise members could export and back up their criminal spoils—stolen personal and financial information—directly to Google Drive.



57. Google identified and blocked the Enterprise account used to support this feature, effectively deactivating it for now.

The Outsider Enterprise

58. The Outsider Enterprise includes several connected groups of criminals that design and implement complex criminal schemes targeting the general public. While different members of the Enterprise may play different roles in these schemes, they all collaborate to enable and

execute phishing attacks using Outsider. None of the Enterprise's schemes can generate revenue without collaboration and cooperation among the members of the Enterprise. All of the groups are connected to one another, including through their use of Outsider and the online Telegram community the Enterprise administers to enable the software's use. Although certain Enterprise members may serve multiple roles, the Enterprise is generally composed of members who participate in the following groups:

59. **The Developer Group.** The Developer Group supplies the phishing software and templates. It includes the individuals or entities that developed Outsider by designing the system's software, architecture, and user interface, writing code to carry out its functions, and conducting testing. It also includes the individuals or entities that continue to maintain and upgrade all the foregoing.

60. The Developer Group constantly creates templates to target new companies and victims. This group is also responsible for providing ongoing maintenance and updates to Outsider—including adding features such as the database backup function that integrated Google Drive's cloud storage function into the Outsider software. Other updates are aimed at hardening Outsider's infrastructure to evade detection—not only by law enforcement and the industry, but also by other cybercriminals seeking to steal Outsider code (rather than license the software) to perpetrate their own scams.

61. One of the members of the Developer Group is an individual or group of individuals operating the Telegram account @sinkinto01. This account is connected to the historical Telegram account @chenlun—an account associated with an earlier version of the Outsider software. In the

fall of 2023, @chenlun's phishing activity was exposed by a cybersecurity researcher,[13] causing @chenlun to deactivate that Telegram account and activity on the prior Outsider software to decline.

62. In May 2025, the person or people behind @chenlun reemerged using the Telegram account @sinkinto01[14] to announce they would be coming out of retirement and releasing the current iteration of the Outsider software.

63. The @sinkinto01 account released the current version of Outsider in July 2025. Since then, @sinkinto01 has issued at least 75 version updates that have upgraded the software's features, provided performance enhancements, fixed bugs, and made other adjustments to evade fraud detection.

64. Enterprise members who purchase a license to use Outsider can connect with other members of the Enterprise who have the necessary expertise to execute particular phishing schemes.

65. **The Data Broker Group.** Members of the Data Broker Group provide lists of targets.

66. These individuals or entities supply curated lists of potential victims' contact information to other members of the Outsider Enterprise, ensuring that Enterprise members have the means to reach a wide number of targets in locations relevant to each particular phishing scheme.

---

[13] *See* Brian Krebs, *Phishers Spoof USPS, 12 Other Natl' [sic] Postal Services*, Krebs on Security (Oct. 9, 2023), https://tinyurl.com/37nf7eyd.

[14] The pinyin transliteration "chenlun" roughly translates to "sink into"; the same Chinese characters are used in both account names. The username @sinkinto01 may also be transliterated as @chenlun01, but most auto-translation functions depict the former name. Google has done the same.

67. Data brokers amass these bulk sets of contact information by mining a variety of sources, including public records, social media, and data breaches.

68. One of the Enterprise members in this group goes by the alias "Nan'an Overseas Data" and uses the Telegram account @heitao888999. This member provides global contact information of potential victims to other members of the Enterprise.

69. **The Spammer Group.** Members of the Spammer Group provide the tools to send fraudulent text messages in bulk.

70. Large-scale smishing schemes require infrastructure to facilitate sending thousands of text messages simultaneously. To do so, the Enterprise needs banks of smartphones, SIM cards, modems, and services that function as the equivalent of call centers to support the data demands of sending mass text messages.

71. The Spammer Group provides these resources to other members of the Enterprise. For example, an individual or group of individuals acting under the Telegram usernames @bailiworking and @adc88adc arrange the sending of bulk messages—including via RCS, SMS, and Google Chat—to potential phishing victims.

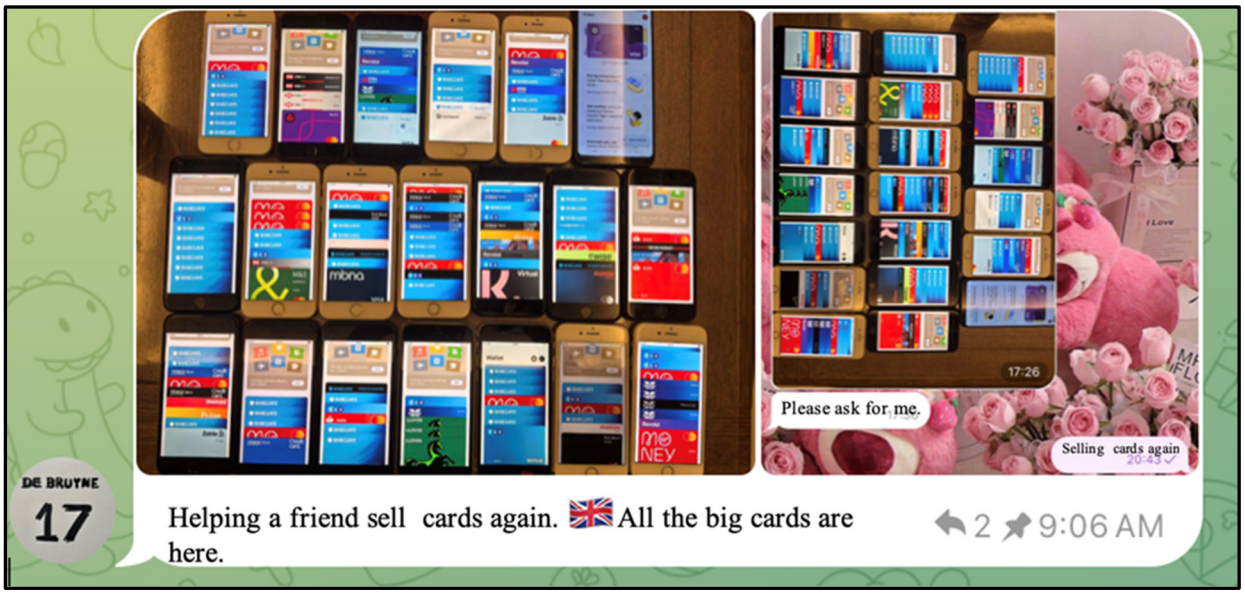
72. The @bailiworking account also helps other Enterprise members engineer phishing messages so that the messages appear to originate from any number the scammer chooses, in order to make them appear legitimate or familiar.

73. **The Theft Group.** Members of the Theft Group help monetize stolen information and launder stolen money.

74. Once members of the Enterprise have successfully 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/or acquire additional victim information.[15] Using Outsider's digital wallet functionality, the Theft Group can also load stolen payment cards to digital wallets like Google Wallet as well as resell the card information or use it to make purchases.

75. For example, a member acting under the Telegram account @yy0205 facilitates the sale of stolen credit cards. On October 14, 2025, @yy0205 posted the following photographs of cell phones loaded with phished credit cards advertising the cards for sale.



76. Other members of the Theft Group help monetize phished credentials. For instance, an individual or group of individuals operating the Telegram account @FHER777 sells stolen verified account credentials obtained by phishing. There are markets for stolen credentials for use at popular retail stores and online services, including Walmart, Uber, Uber Eats, and DoorDash, and members of the Enterprise sell phished credentials into those markets for payment or exchange.

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

77. The Theft Group also launders stolen money for the Enterprise's continued use. For example, Telegram account @yy0205 helps scammers secure point-of-sale machines to launder funds from stolen credit cards. On October 17, 2025, @yy0205 offered point-of-sale machines that take credit card payments, as shown in the picture below. These machines can act as intermediaries—taking payment from the stolen card into a dummy "merchant" account, from which the scammer can quickly withdraw funds, thereby obscuring the original source.

78. **The Telegram Group.** The Telegram Group runs an online community designed to facilitate collaboration among the Enterprise and recruit new members.

79. Part of the Outsider software's appeal is the ease with which someone with limited technical expertise—like many members of the Enterprise—can purchase the software, execute various phishing attacks, and, upon purchase, meet other members of the Enterprise who are proficient in other areas. The online forums run by the Telegram Group make this possible.

80. The Telegram Group uses at least four Telegram channels to facilitate the Enterprise's collaborative use of Outsider to carry out phishing attacks: @OutsiderCodeBot; @sinkintopd; @sinkintojl; and the "Outsiders Member Group." These Telegram channels serve a variety of purposes to execute successful phishing schemes, including licensing the Outsider

software; connecting Enterprise members to one another based on their specific specialties; training Enterprise members; and coordinating strategies among members to optimize phishing campaigns.

81. *@OutsiderCodeBot Channel.* The Enterprise sells Outsider licenses on a Telegram channel called @OutsiderCodeBot, set up by @sinkinto01, through a "self-service ordering bot." Members may purchase licenses with a duration of a week or month. These licenses cost $88 and $200, respectively, which members pay for in the digital currency, USDT. From August 2025 to March 2026, Enterprise members purchased more than 250 licenses. One license allows a member to create hundreds of websites that could steal thousands of credit cards each day.

82. Beyond selling and marketing Outsider, the @OutsiderCodeBot channel also connects Enterprise members to each other. For example, this channel linked users to @adc88adc—a member of the Spammer Group that provides mass texting capabilities, as noted above. This channel also displays a message directing Enterprise members to an @outsiderserverbot Telegram channel. There, Enterprise members can request assistance purchasing Google Cloud to host the phishing websites they create with Outsider. This Google Cloud feature also underscores the scale of what Outsider offers—the possibilities for generating phishing websites, especially with AI, are endless, necessitating Cloud-based storage.

83. *@sinkintopd Channel.* The @sinkinto01 account refers to the @sinkintopd channel as the "development diary" channel. Here, members of the Development Group send other Enterprise members updates and tutorials on the Outsider software. The @sinkinto01 account has posted at least 175 messages and 13 tutorial videos to the channel explaining different features of the Outsider software.

84. In an August 2, 2025, video posted by @sinkinto01 to the channel, users are instructed to copy the code from an Outsider template, paste it into Gemini, and prompt Gemini to rewrite functions, change the look of the page, add fields, or otherwise make the template site more convincing. Another video demonstrates how to copy Gemini's modified code back into Outsider to replace or update the phishing page. Still other videos provide similar instructions for other AI platforms.

85. *@sinkintojl Channel.* The @sinkintojl channel is an Outsider community discussion group where members post about phishing-related issues and can find resources to develop and execute phishing attacks.

86. Here, members offer to sell global SMS data, credit card data, stolen Gmail account information, and personal information like passports and other identification documents. As shown in the picture below, on November 10, 2025, users made posts offering to sell stolen Gmail addresses, global SMS data, and credit card data. Others posted in search of "SMS routes for Colombia, Mexico, [and] Chile."

87. The @sinkintojl channel has four administrators: @sinkinto01, @bailiworking, @yy0205, and @FHER777. Administrators have authority to invite, ban, and remove members and to moderate content by deleting messages, "pinning" important messages, and controlling other chat settings. Each of these administrators serves as a gateway to additional Telegram channels with phishing resources, and they leverage those channels to recruit new Enterprise members.

88. The @bailiworking account's Telegram biography links to the channel @waterworking001. The @bailiworking account uses @waterworking001 to advertise Outsider and has offered the account as a point of contact to purchase an Outsider subscription.

89. The @yy0205 account's profile links to the channel @shiqi0205, which contains discussions about phishing and has been used to recruit Enterprise members. In a September 29, 2025, post, @sinkinto01 promoted Outsider on the @shiqi0205 channel, highlighting that the software allowed users to "freely import any website for customization." Both @sinkinto01 and @bailiworking are also administrators of the @shiqi0205 channel.

90. The @FHER777 account operates several Telegram channels, including @zhuoyue_logs, which offers access to stolen accounts, and @Zhyuebot, which can be used to swap cryptocurrency for USDT—the cryptocurrency Enterprise members need to purchase an Outsider license.

91. The posts mentioned in paragraphs 86 and 89 were also made in either the @sinkintojl channel or one of the channels connected to the @sinkintojl channel through an administrator's biography. This consolidation of resources enables the Enterprise to develop and execute large-scale attacks and expand its reach.

92. *Outsiders Member Group Channel.* The Outsiders Member Group channel is an invite-only channel for Enterprise members who have purchased Outsider. The @sinkinto01, @bailiworking, and @FHER777 accounts are members of this group, along with more than 160 other Telegram accounts. The group includes conversations among Enterprise members about strategies for optimizing their phishing campaigns, and coordination among the different groups to execute attacks. The @sinkinto01 account answers member questions, and various other members of the group also provide tips and tricks.

93. 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 discuss specific Outsider phishing schemes. Although these schemes are plainly criminal, the Enterprise brazenly coordinates its efforts in open and largely uncoded discussions on Telegram.

94. For example, on February 24, 2026, a member of the Data Broker Group advertised that they were "open for e-commerce fish trading in CA and the US"; *i.e.*, selling contact information for U.S.-based victims. On the same day, a member of the Scammer Group asked, "does anyone have any Chilean fish?"; *i.e.*, looking for potential victims in Chile.

95. Members of the Enterprise leverage this online community to access resources and expertise necessary to carry out their criminal schemes. Through their Telegram groups, Enterprise members coordinate with each other to recruit and train new members of the Enterprise, generate phishing strategies and tactics, select phishing targets, and coordinate and execute phishing attacks.

* * * *

96. The Developer Group created the software and relays information about software updates to other members of the Enterprise. The Telegram Group markets Outsider to recruit new members to the Enterprise, and through the Telegram 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 victims' information in hand, the Theft Group sells or uses that information and helps to launder ill-gotten funds.

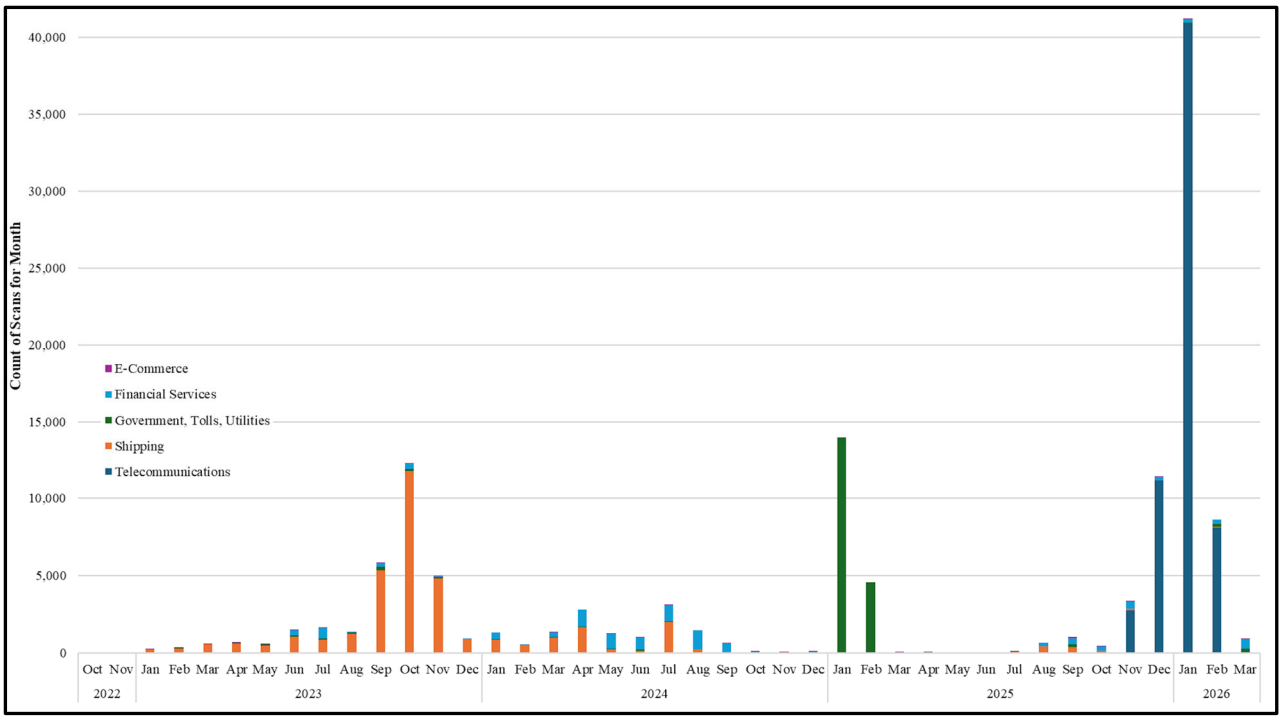
Fraudulent Schemes Perpetrated by the Outsider Enterprise

97. The Outsider Enterprise deploys sophisticated schemes targeting multiple industries. Many of these schemes are executed in similar ways.

98. First, an Enterprise member creates and customizes a phishing template using Outsider, as described in detail in paragraphs 36–45 above. Next, the phishing site is deployed to targets through "bait" messages or internet advertisements. The Enterprise member can then monitor the phishing attack on Outsider and collect sensitive personal and financial information that can be monetized.

99. This simple framework for phishing attacks can be adapted to mimic different industries. As public awareness of a particular type of phishing attack rises, the efficacy of the attack declines. The Enterprise then responds by shifting its focus to a different industry, allowing it to continue successfully duping the public.

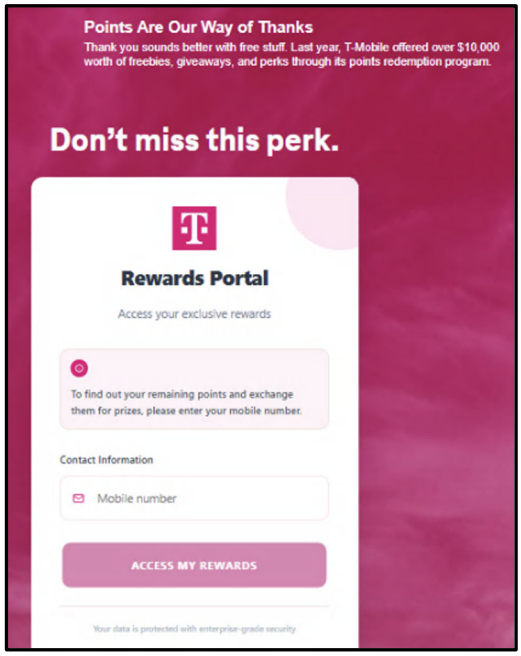
100. In January 2023, using the prior iteration of Outsider, scammers predominantly targeted shipping companies. As consumer protection campaigns raised awareness of those package delivery scams, in 2024, scammers started to target brokerage firms. In early 2025, the scams began to target toll authorities. Now that there is widespread awareness of each of those types of scams, the Outsider Enterprise has pivoted yet again to the latest set of targets—telecommunications companies. The graphic below demonstrates the industries targeted by phishing scams, created by Outsider and its predecessor, over time.



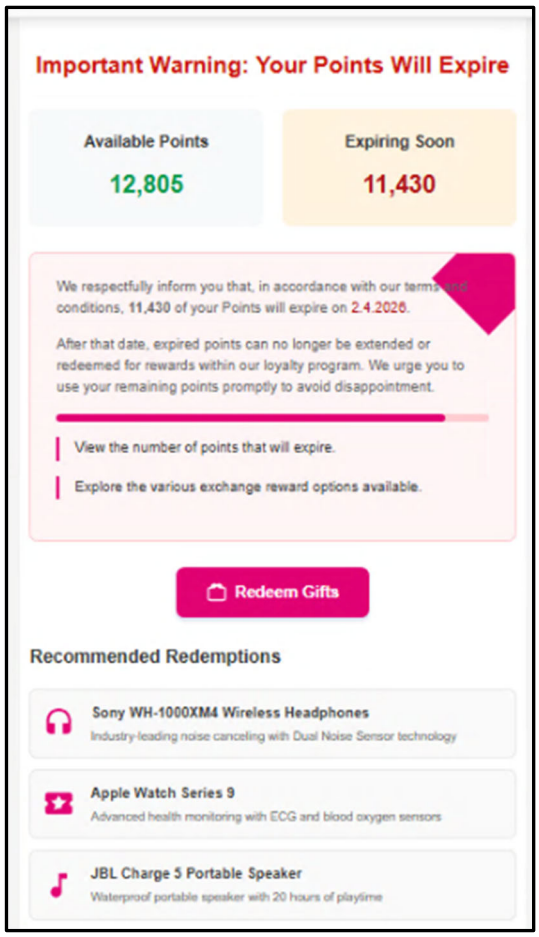
101. Notwithstanding its current focus on telecommunications, the Outsider Enterprise continues to execute a variety of schemes—each tailored to a particular industry but generally following the same core playbook. Five of the most commonly used schemes executed by the Outsider Enterprise are the Telecommunications Scheme, the Brokerage Firm Scheme, the Delivery Scheme, the Toll Scheme, and the E-Commerce Scheme.

102. **Telecommunications Scheme.** The Outsider Enterprise's impersonation of major wireless carriers is its fastest growing scheme, leveraging the names of major wireless networks and cellular providers to reach more victims. Currently, Enterprise members are using Outsider-generated templates targeting telecommunications companies at a rate that far exceeds all other schemes. Because this scheme exploits the trusted relationship between consumers and their wireless carriers, it has proven especially effective at deceiving victims who might otherwise recognize a phishing attempt.

103. This scheme generally begins with a text message notifying the victim of available "points" for redemption under a rewards program ostensibly offered by their wireless service provider. The message includes a link to what appears to be the wireless service provider's "Rewards Portal," depicted below.

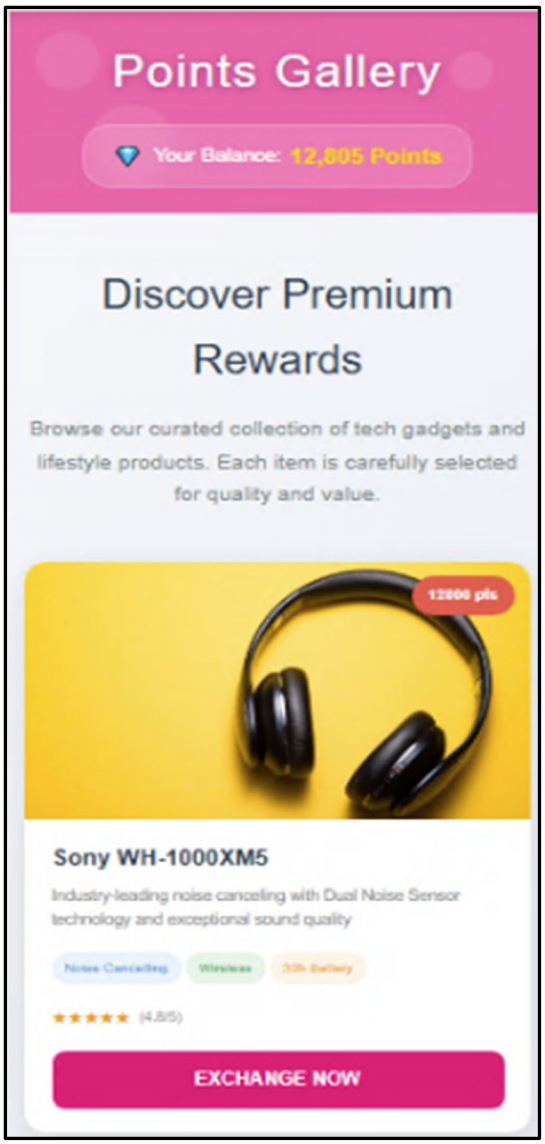


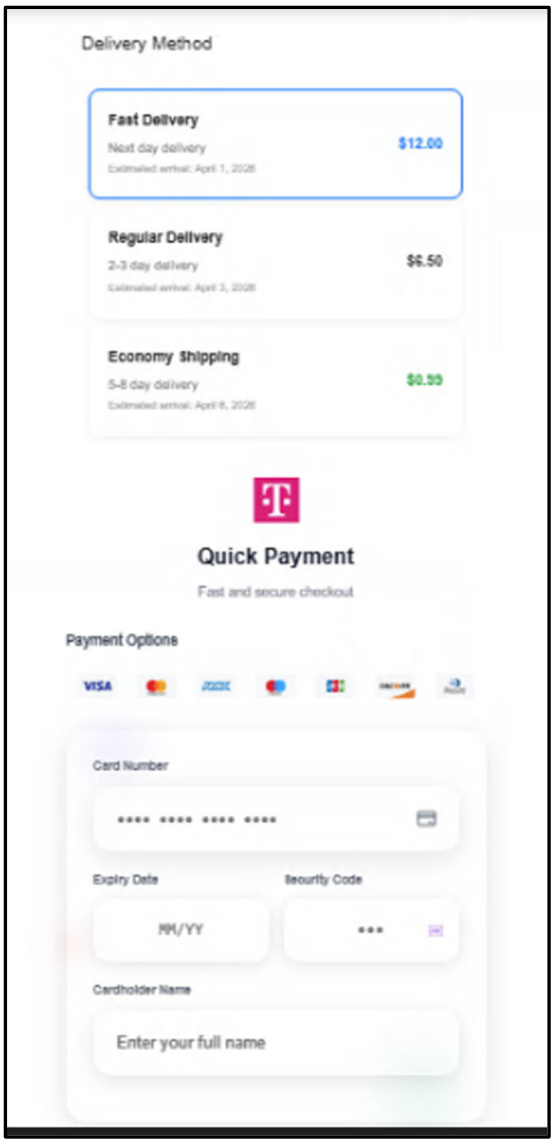
104. After entering their phone numbers, victims are brought to a rewards page, similar to the one shown below, that encourages them to redeem points. To create a sense of urgency, these pages prominently display a warning that the points are about to expire, typically showing that nearly all accumulated points will expire soon.



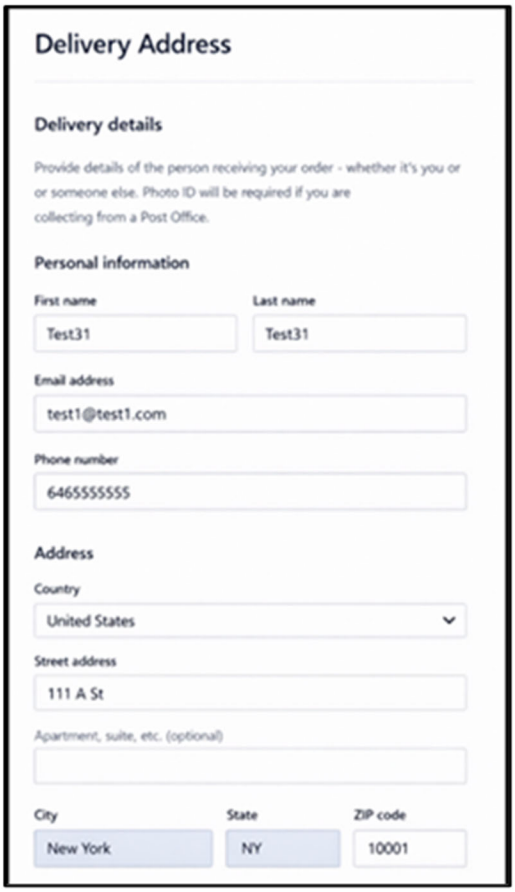
105. The rewards page often includes a "Redeem Gifts" option along with a "Recommended Redemptions" section designed to entice the victims with high-value items. As shown in the example above, these can include products such as expensive Bluetooth headphones, the latest Apple Watch, or a portable speaker.

106. When victims click the "Redeem Gifts" button, the phishing site directs them to a gallery of products that can be purportedly redeemed with their points at no cost. Victims are told all they need to pay is the cost of shipping. This, of course, is where financial information is entered and stolen. After selecting an item and confirming the fake exchange, victims are directed to a payment page where they are prompted to select a shipping option and to enter their payment information, as shown below.





107. Believing they are receiving high-end products in exchange for a small shipping fee (ranging from $0.99 to $12.00), victims input their payment information. Victims are then directed to a webpage, as shown below, prompting them to enter their shipping information.

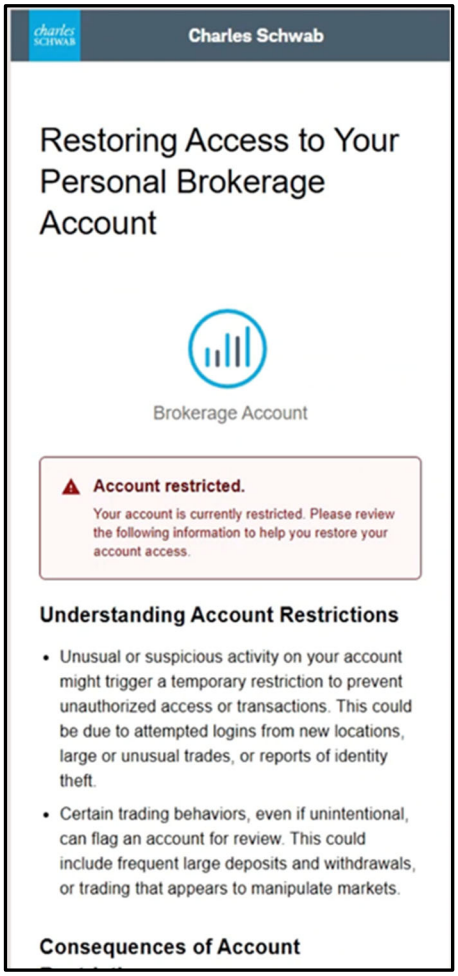


108. Unbeknownst to the victims, as they enter financial and personal information, Outsider captures it in real time by tracking their keystrokes. Victims thus need not actually submit the payment for the scammer to procure their payment information. From an Outsider account, the Enterprise can compile a full profile on victims in real time—including their name, email address, shipping address and financial information.

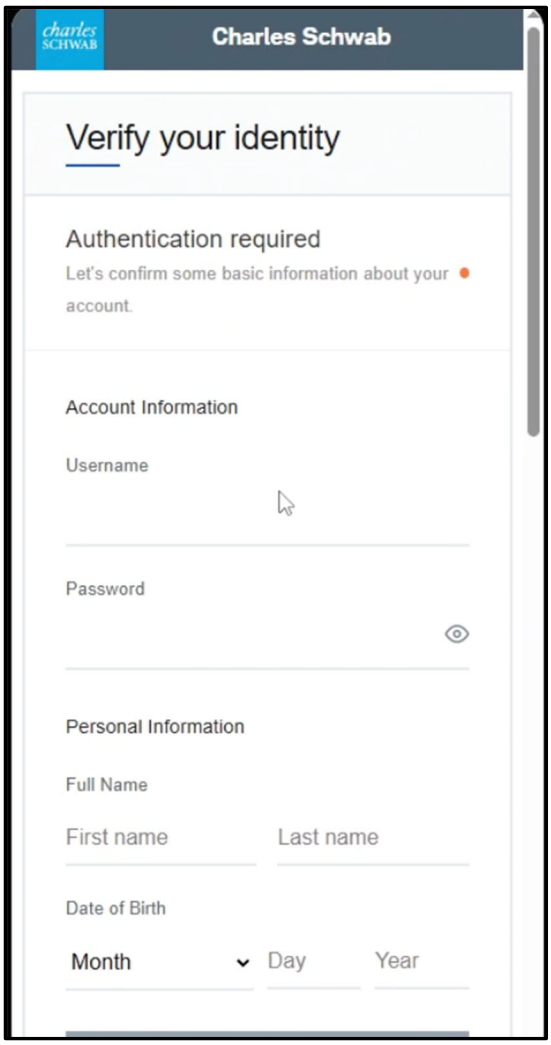
109. Members of the Enterprise collaborate to execute the attack. The Data Broker Group provides lists of mobile phone numbers to the Spammer Group. The Spammer Group then sends the fraudulent 'rewards' messages in bulk—via RCS, iMessage, and SMS—to thousands of targets. Enterprise members can then monetize the stolen information through the Theft Group, either by selling digital cards that the Outsider software automatically generates or by selling the victims' financial and personal information directly.

110. **Brokerage Firm Scheme.** The Enterprise also uses Outsider to impersonate brokerage firm websites and phish for victims' login credentials.

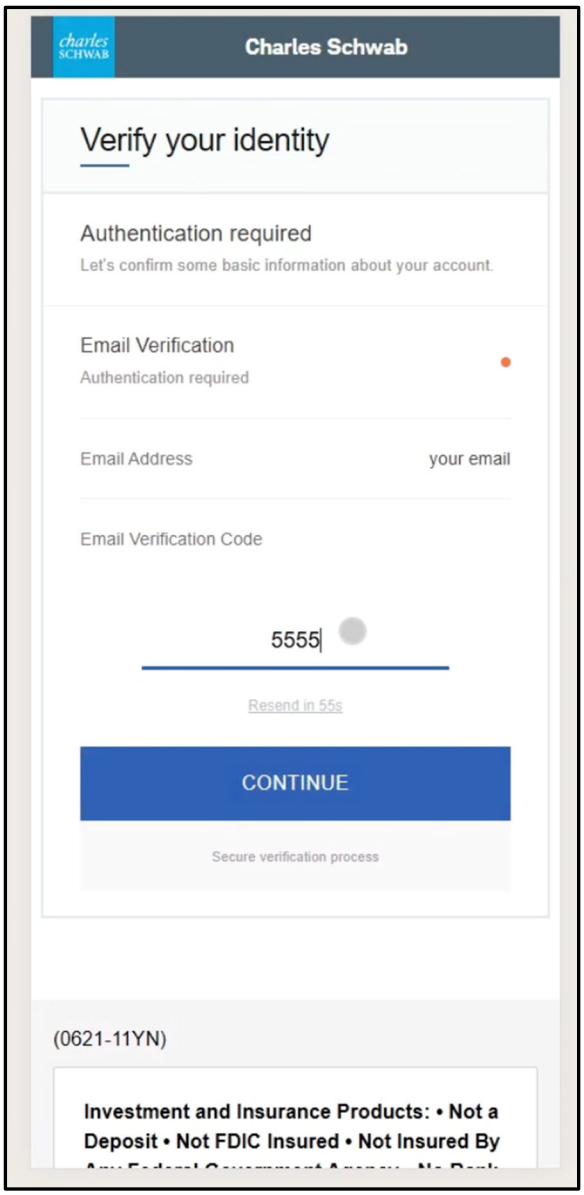
111. In this scheme, the phishing webpage tells the target that their account has been restricted, as pictured below.



112. It then prompts the user to "verify their account," providing the target with various options for verification, each requiring them to input different personal information. Believing the website to be genuine, the victim inputs their account information into the form on the website, as shown below.



113. Once a victim attempts to access their account on the pages pictured above, they are directed to a fictitious MFA phishing page, prompting them to enter a code to verify their account. The victim will find a code available for use on their device because, at the same time that the victim is "logging in" to the fraudulent site, members of the Enterprise are using the same information to log into the real bank—prompting the issuance of a code.



114. As described above, once the victim supplies the MFA code, the scammer uses the victim's provided login information and MFA to complete the login process.

115. A tutorial video posted by @sinkinto01 on Telegram showcases Outsider's ability to create fraudulent versions of the websites of major U.S.-based brokerage firms. The tutorial trains members of the Enterprise to use Outsider and to deploy phishing attacks through their Outsider accounts. Members of the Enterprise can then access that information by logging into

their Outsider accounts, as the platform provides the functionality to collect and organize victims' stolen data.

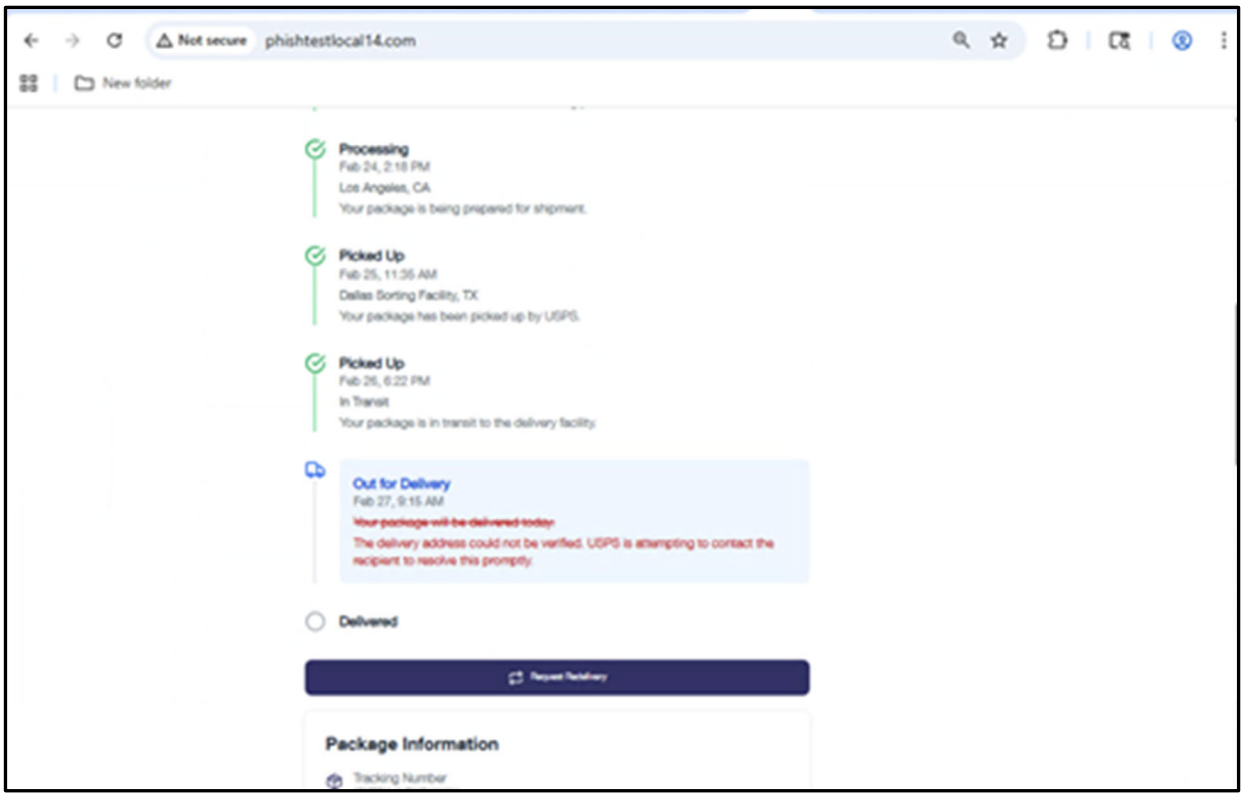
116. Once Enterprise members have the victims' credentials, they can monetize them in a variety of ways. For example, the scammers can sell the credentials, or they can use the credentials to access victims' brokerage accounts, liquidate assets, and steal the funds.

117. One option for monetizing this scheme, which has grown in popularity, is an online version of "pump and dump." To carry out this version of the scheme, the scammer first purchases shares of a particular stock in their own name. After collecting a victim's brokerage account credentials through the phishing attacks described above, Enterprise members purchase stock in that victim's name to artificially inflate ("pump") the stock price. They then repeat this process with other victims until the stock reaches a target price. Once it does, the Enterprise members sell ("dump") their original holdings, reaping substantial profits and saddling the compromised account holders with losses.

118. "Pump and dump" schemes are most effective when criminals coordinate their attacks. The more scammers that pump the stock price, the more quickly the stock price rises. Members of the Enterprise can coordinate these attacks using the Telegram channels administered by the Telegram Group to launch these attacks on larger scales than they could alone.

119. **Delivery Scheme.** The Outsider software also facilitates scams that target the United States Postal Service ("USPS") and other national and international shipping companies.

120. From the victims' perspective, the USPS scam begins with a fake USPS text message purporting to notify a victim of an issue with a package—for example, that a delivery was missed. The message includes a link to a website created using Outsider, like the one depicted below, ostensibly for the victims to reschedule their delivery.

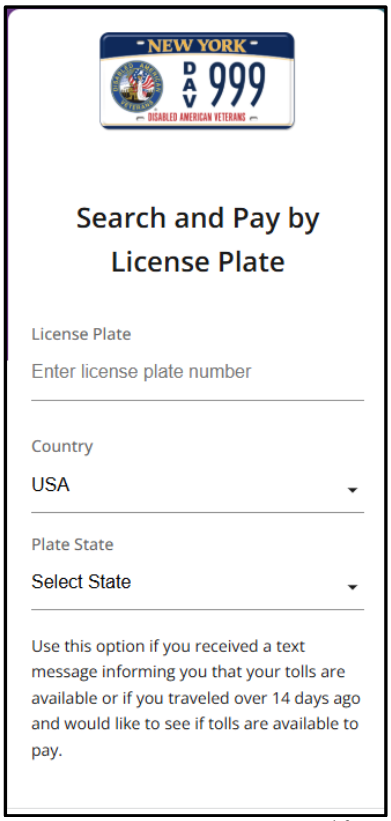


121. If victims clicks the link, they are directed to a fake USPS website that requires payment of a small redelivery fee. Of course, the original text message was a ruse; there is no re-delivery to schedule, and "payment" of the "fee" only channels the victim's payment information to the Enterprise.

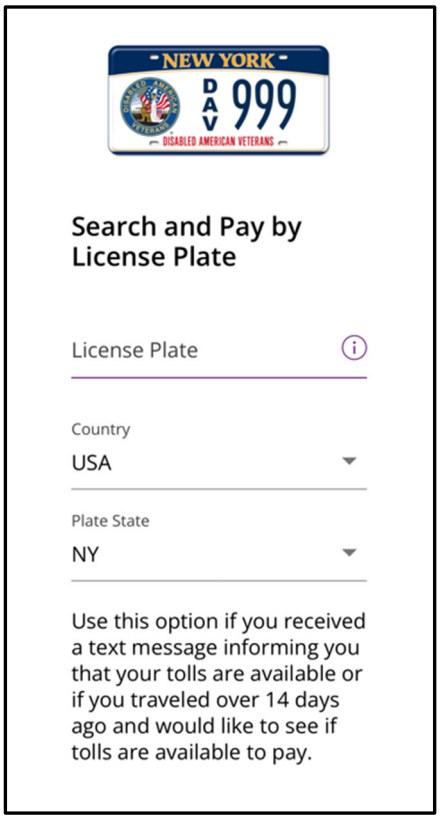
122. **Toll Scheme.** Similar to other large phishing kits, the Outsider software supports scams involving text messages concerning toll violations and tickets.

123. Outsider includes at least 102 templates for fraudulent government websites that target victims in the United States. For example, Outsider offers a fake version of the website for E-ZPass, New York's popular toll-paying system. It also offers a template for the official New York City government website.

124. The Outsider templates are nearly indistinguishable from the legitimate websites they are designed to mimic. Reproduced below, for example, are the Outsider version (left) and the real version (right) of the E-ZPass New York website.



Outsider Template[16]



Real Website[17]

125. As outlined above, when victims type their personal data into the fake site, Enterprise members can track the inputs in real time.

126. This scheme also relies on coordination among members of the Enterprise. For example, the Data Broker Group provides the Spammer Group with potential victims' phone

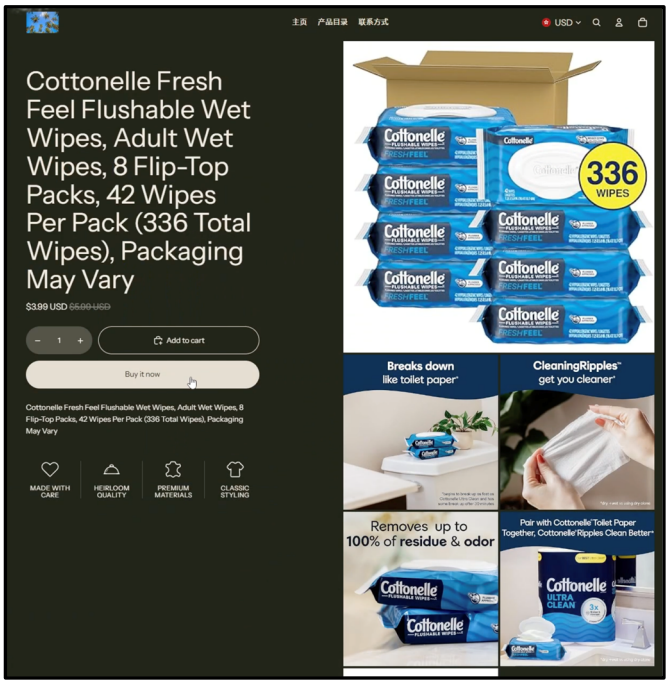
[16] This is a screenshot of Outsider's template for E-ZPass New York on or around March 10, 2026. NAXO Declaration in Support of Plaintiff's Motion for TRO and Order to Show Cause ¶ 13, Figures 13, 14.
[17] This is a screenshot of the E-ZPassny.com website as it appeared on or around April 2, 2026. Wayback Mach. Internet Archive, E-ZPass N.Y. Service Ctr., https://tinyurl.com/23tasnt6.

numbers, and the Spammer Group then sends SMS or RCS messages in bulk to the phone numbers. In this example, the Spammer Group would use geolocation information to match victims with the appropriate local governments or toll collection agencies.

127. The targets then receive text messages purporting to provide notice of past-due toll invoices or tickets, along with links to the fraudulent websites. Like the Brokerage Firm and Delivery Schemes, the Toll Scheme invites victims to input personal payment information, such as their credit card numbers, to pay the purported tolls.

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

129. **E-Commerce Scheme.** The Enterprise can also use Outsider to create e-commerce scams to defraud victims. Outsider enables the Enterprise to build fake e-commerce websites, like the one pictured below. This particular website displays a listed product, Cottonelle Fresh Feel Flushable Wet Wipes.



130. Product phishing pages like these can be listed on legitimate e-commerce websites or may function as a standalone phishing website. Victims usually arrive at Enterprise-created e-commerce sites through searches on the legitimate e-commerce site or by clicking online advertisements.

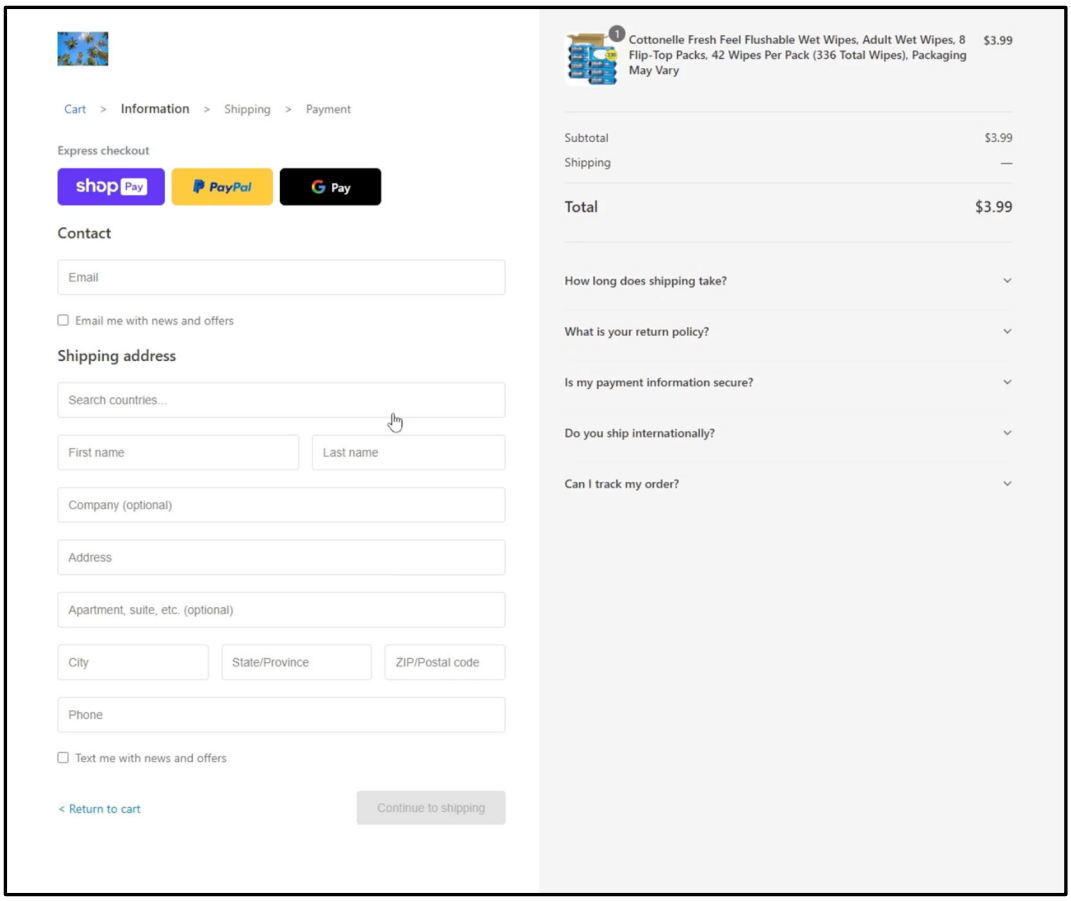
131. The Enterprise uses online advertising platforms to create ads that link to its fraudulent e-commerce websites.

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

133. The Enterprise then uses its advertising accounts to place online ads, with links to fraudulent websites, on websites and on social media. If a victim clicks the advertisement, they are directed to the fake website. When the product is selected and the victim attempts to "check out," they only relay their payment information to the Enterprise, and no product is ever sold or delivered.

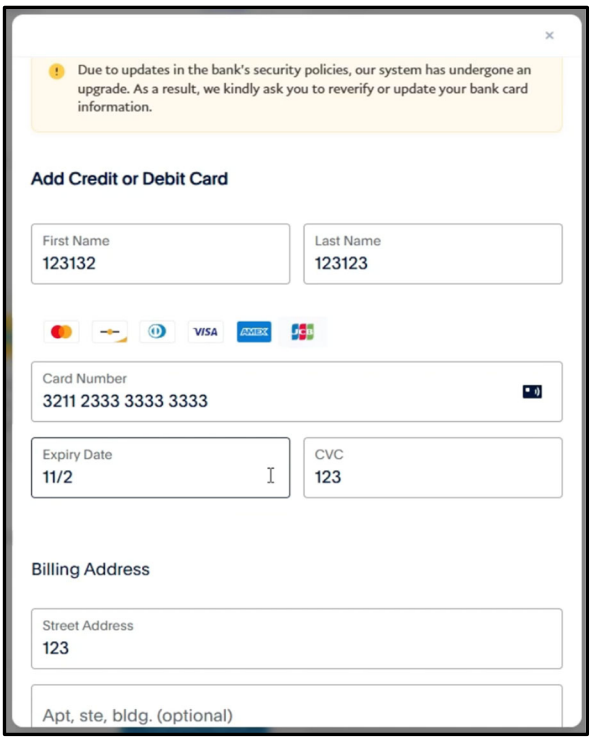
134. The Enterprise can design the e-commerce website to offer a wide variety of products, ranging from wet wipes to phone accessories to reusable water bottles and more. A tutorial video posted by @sinkinto01 shows how the e-commerce scam works, using a webpage purporting to sell flushable wet wipes.

135. When a user attempts to purchase a listed product, they are directed to a page that prompts them to input payment information and a shipping address, as shown below.

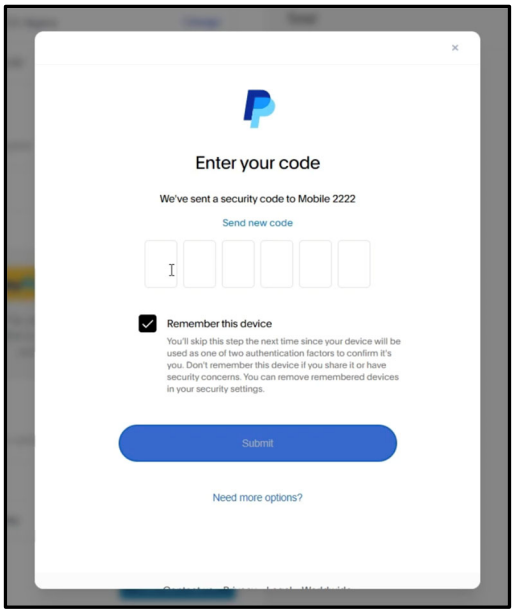


136. The phishing website featured in the tutorial video includes text stating "express checkout" followed by the logos of several reputable electronic payment systems, including Google Pay and PayPal. Indeed, when building a fake website, Outsider provides the option to customize websites by adding Google Pay as an option.

137. The tutorial video shows that when the victim clicks the PayPal payment option, a login page appears, prompting the victim to enter an email address and password. When they do, the "site" displays an error message and requests that the victim enter their credit card information. The types of payments that are "accepted" by the website include "Mastercard, Discover, Diners Club, Visa, American Express, and JCB." This feature of Outsider phishing websites is specifically designed to give the target a sense of false comfort by reciting reputable payment platforms.



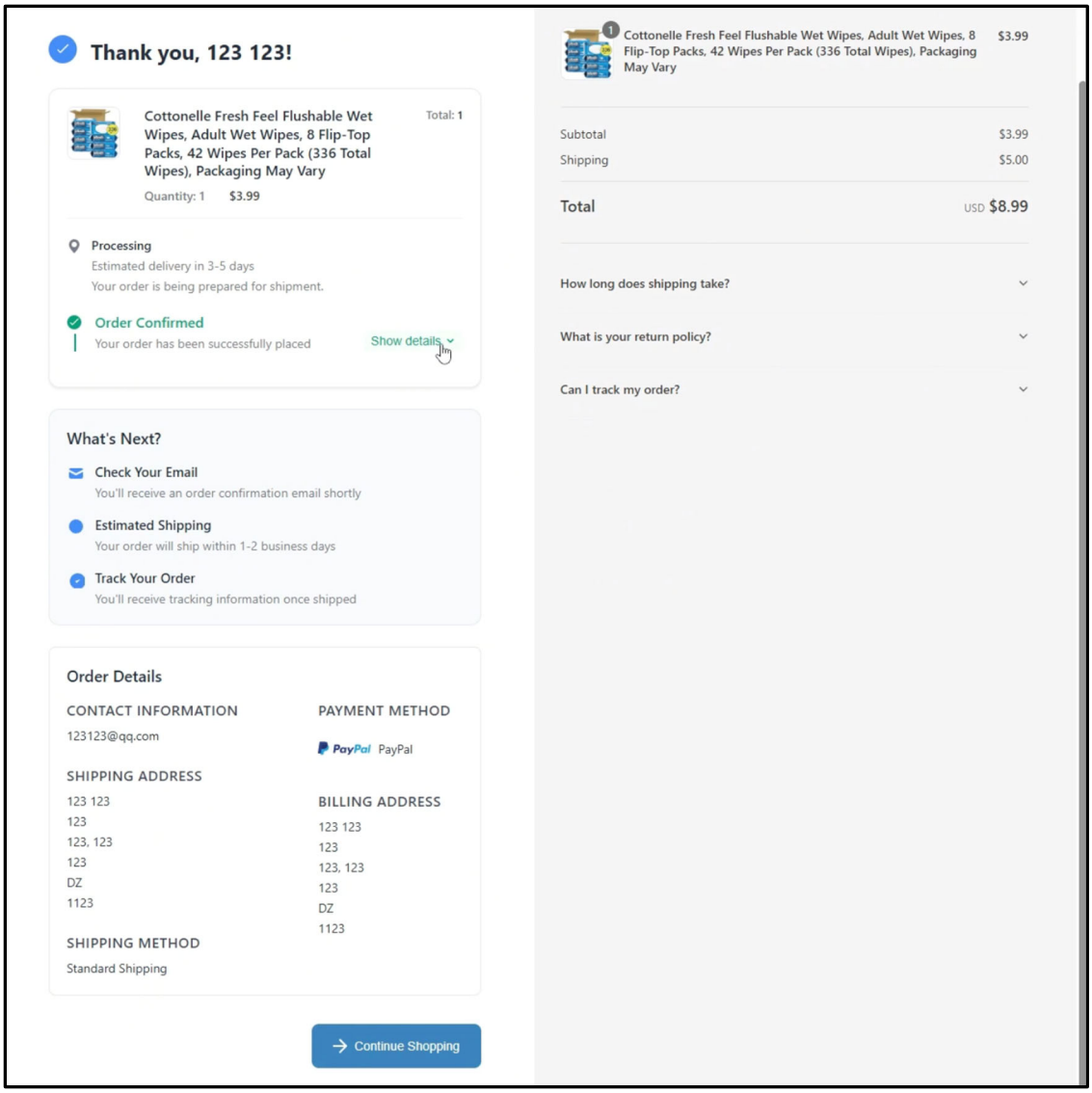
138. Once the victim inputs and submits their credit card information, they are directed back to a purported PayPal screen, which prompts them to enter a security code, as shown below.



139. Because the scammer previously received the victim's PayPal account credentials, as described in paragraph 133, the scammer can attempt to log into the victim's PayPal account,

causing an MFA code to be sent to the victim's phone. The victim receives the MFA code and enters it into the phishing website, allowing the Enterprise member to access the victim's PayPal account. The same process occurs if the victim selects Google Pay as a payment option.

140. Once the scammer has all of the information needed to access the victim's account, the scammer can send the victim a fake confirmation page, as shown below.



Harm to Google, its Users, and the Public

141. The Outsider Enterprise has victimized well over 100,000 people, swindling innocent victims out of millions of dollars, and continues to create new phishing sites. The prior

version of the software was responsible for the theft of at least 36,000 payment cards issued by financial institutions in 95 countries. In the five-month period from November 2025 to April 2026 alone, Google detected more than 1.59 million webpages linked to the Outsider Enterprise. This number shows the Enterprise's staggering scale and productivity. Though Google and other companies are working to thwart phishing attacks, the Enterprise launches thousands of new sites every day.

142. The Outsider Enterprise harms its victims by stealing their personal information, their money, and access to their accounts.

143. The Outsider Enterprise harms Google by damaging customer trust and goodwill in the Google Marks and services the Enterprise cites for credibility, and the tools it abuses in the development and execution of its schemes. Google suffers reputational harm when consumers associate its Marks, platforms, and the internet generally with fraudulent schemes. The Enterprise's abuse of Google services also forces Google to invest significant time and resources in detection and remediation efforts.

144. In just a two-week period from May 18 to June 1, 2026, Google received more than 55,000 reports—including from users in the United States—of suspicious messages transmitted over Google Messages, including reports of fraudulent phishing messages received from the Outsider Enterprise attempting to lure victims into clicking links to fraudulent websites. For example:

a. On June 1, 2026, a U.S-based Google Messages user reported receiving a phishing message from Defendants that stated, "Your … account currently holds 18,400 points, scheduled to expire on May 26, 2026. Per the program terms, unused points will be removed automatically after this date and cannot be reinstated," followed

by a link to a website domain created through Outsider to spoof the website of a U.S.-based wireless service provider.

b. On May 31, 2026, a U.S.-based Google Messages user reported receiving a phishing message from Defendants that stated, "Your vehicle registration renewal is suspended due to unpaid tolls. Use this official link to pay," followed by a link to a website domain created through Outsider to spoof the website of a Michigan state agency.

c. On May 26, 2026, a U.S.-based Google Messages user reported receiving a phishing message from Defendants that stated, "We've noticed you've accumulated a significant number of reward points in your … Rewards account. Please be sure to check the expiry date of your points to avoid them expiring," followed by a link to a website domain created through Outsider to spoof the website of a U.S.-based wireless service provider.

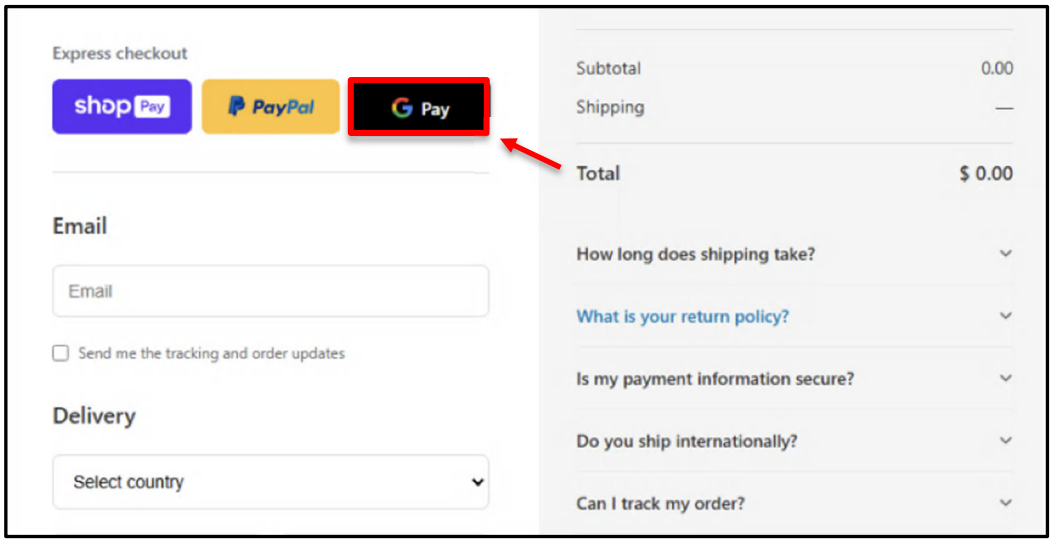
d. On May 28, 2026, a U.S-based Google Messages user reported receiving a phishing message from Defendants that stated, "We attempted to deliver your package on May 19, but were unable to complete the delivery. A signature was required at the time of delivery, and no one was available to sign for the item at the address on file. To avoid any further delays, please select one of the following options," followed by a link created through Outsider to spoof the website of USPS.

e. On May 20, 2026, a U.S.-based Google Messages user reported receiving a phishing message from Defendants that stated, "We encourage you to take advantage of these rewards before time runs out. … This is a friendly reminder that your 11,430 … reward points will expire on December 24, 2029[.] As stated in our

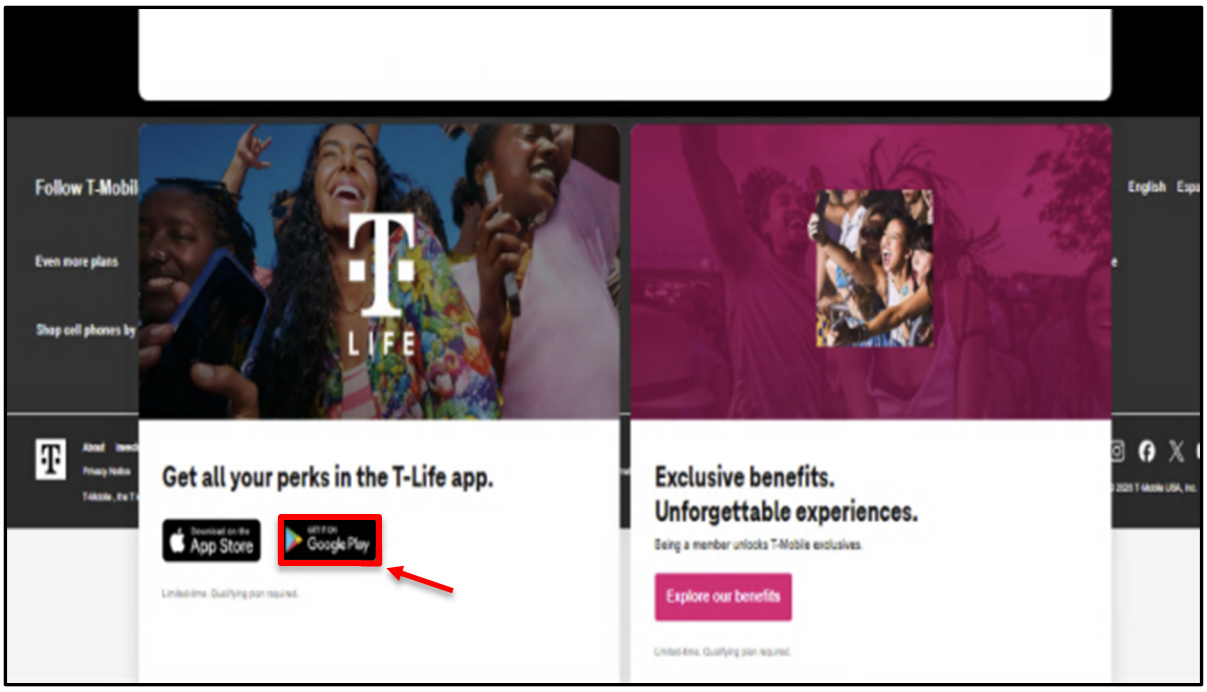
terms, any unused points will automatically be withdrawn after this date," followed by a link to a website domain created through Outsider to spoof the website of a U.S.-based wireless service provider.

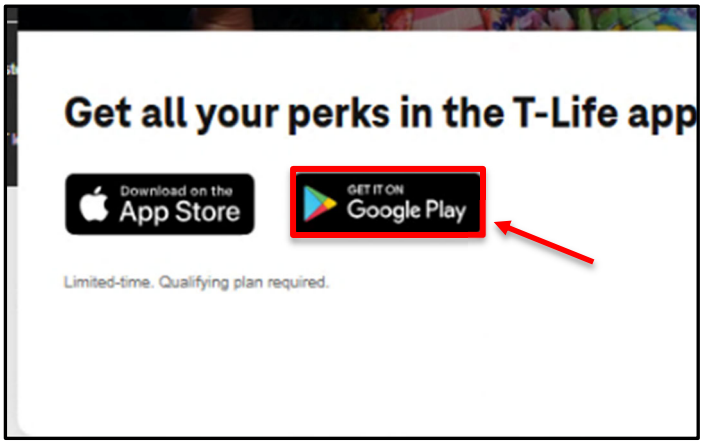
145. Indeed, the Enterprise has created and deployed at least 14 fraudulent website templates featuring Google's branding or logos (YouTube, Google Pay, or Google Play) on the sign-in screen in an attempt to make the fake websites appear legitimate.

146. Some of the fraudulent templates feature the Google Pay logo.

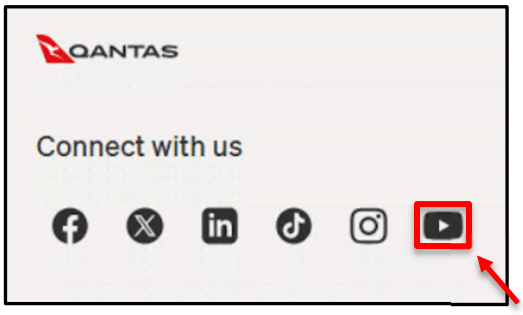


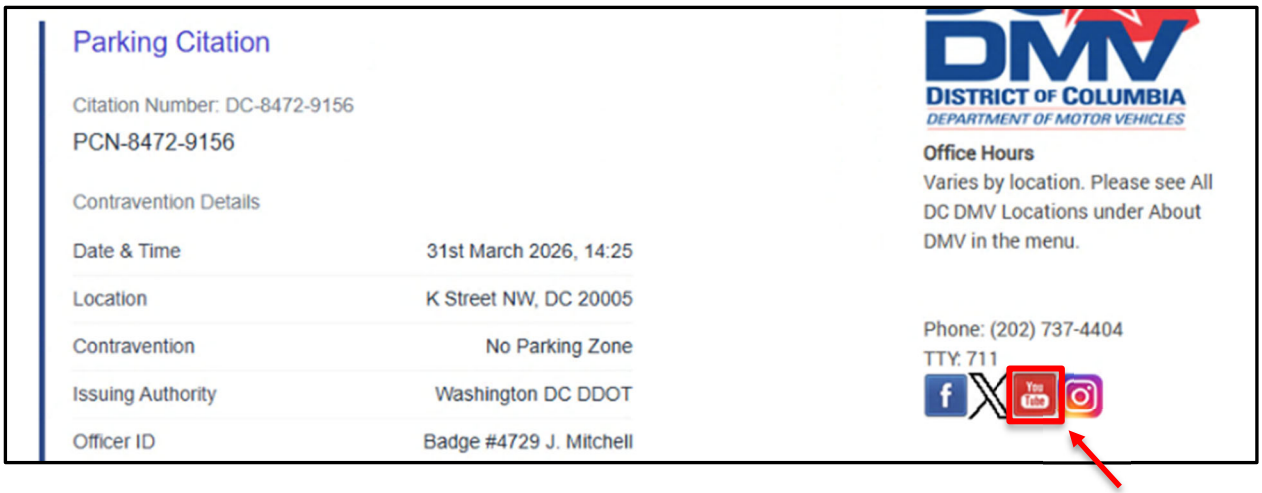
147. Other templates feature the Google Play logo, suggesting that targets can download the spoofed brand's app in the Google Play store.





148. Other fraudulent websites include the YouTube logo, along with the logos of other prominent social media sites, suggesting that clicking the logo will take the user to the spoofed brand's YouTube channel.





149. Victims may view the presence of a Google logo as an indicator that the website is safe or legitimate. The Outsider Enterprise is thus exploiting Google's branding—and the goodwill associated with it—to convince victims to divulge sensitive personal and/or financial information.

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

151. The use of these logos violates Google's guidelines for proper usage of its trademarks and brand features, which bar, among other things, "display[ing] a Google Brand Feature on a site that violates any law or regulation," "display[ing] a Google Brand Feature in any manner that implies a relationship or affiliation with … Google," or "display[ing] a Google Brand Feature in a manner that is … misleading[] [or] infringing."[18] 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.[19]

[18] Google, *Trademark guidelines for proper usage*, Brand Res. Ctr., https://tinyurl.com/24dvmced (last visited June 10, 2026).
[19] Google, *Google Play: Legal and trademarks*, Partner Mktg. Hub, https://tinyurl.com/2yz2mscd (last visited June 10, 2026).

152. The Outsider Enterprise frequently distributes these phishing messages to potential victims using Android devices and Google Messages (through RCS).

153. The Enterprise also has exploited Google Drive by including a "backup feature" in the Outsider software, enabling Enterprise members to export stolen personal and financial data directly to Google Drive. Although Google has now blocked Outsider's access to Google Drive, the feature reflects the Enterprise's deliberate effort to use Google's services to warehouse and manage stolen victim data.

154. And members of the Enterprise procured Google Cloud servers—facilitated through the @OutsiderServerBot channel—to host phishing websites generated using the Outsider software.

155. These uses of Google Drive and Google Cloud violate Google's Terms of Service, which require account holders to agree that they will not be "accessing or using [Google] services in fraudulent or deceptive ways, such as … phishing" or "creating fake accounts."[20] 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.

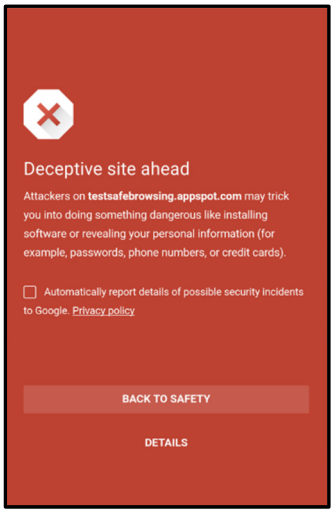
156. The Enterprise's misuse of Google Cloud and Google Drive also violates the Google Cloud Acceptable Use Policy, which prohibits "violat[ing], or encourag[ing] the violation of, the legal rights of others"; "engag[ing] in, promot[ing], or encourag[ing] illegal activity"; and "generat[ing], distribut[ing], publish[ing] or facilitat[ing] unsolicited mass email, promotions, advertisements, or other solicitations."[21]

[20] Google, *Terms of Service*, https://tinyurl.com/ynm67nz3 (last visited June 10, 2026).
[21] Google, *Google Cloud Acceptable Use Policy*, https://tinyurl.com/226jfyap (last visited June 10, 2026).

157. The Enterprise's use of Gemini to create custom shell websites to load into Outsider violates Google's Generative AI Prohibited Use Policy, which prohibits users from "[a]ttempting to generate content to engage in dangerous or illegal activities" and "[u]sing generated content to engage in frauds, scams or other deceptive actions."[22]

158. Google has invested significant resources to combat the Outsider Enterprise's violations and other cybersecurity threats. Since it started tracking Outsider, Google has identified more than 1.59 million webpages associated with Outsider's phishing schemes. Though Google and other companies are working to stop phishing attacks, the Enterprise launches thousands of new sites every day. Indeed, at the peak, Google detected 62,993 new Outsider pages in a single day.

159. As part of its response, Google updated its Safe Browsing catalogue to include these detected webpages and issue warnings when Chrome users attempted to visit them, similar to the below image. After the Safe Browsing warnings went live, traffic to these pages by Google Chrome users plunged dramatically. Users of other web browsers may not see such a warning upon clicking on Outsider phishing webpages.



[22] Google, *Generative AI Prohibited Use Policy*, http://tiny.cc/k7hz001 (last visited June 10, 2026).

160. Google has spent hundreds of hours investigating and remediating Defendants' activities. These efforts are ongoing.

CLAIMS FOR RELIEF

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

161. Google incorporates by reference the foregoing paragraphs (¶¶ 1–160) of the Complaint as if set forth in full.

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

163. 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).

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

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

The RICO Enterprise

166. 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 Outsider Enterprise, have worked together over time to create, control, and use Outsider to execute numerous criminal schemes that harm and threaten to continue to harm Google, its users, and the general public.

167. As described *supra* at paragraphs 58 through 96, 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 Enterprise members, and expanded the scope and range of their activities.

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

169. Defendants constitute an associated-in-fact enterprise within the meaning of 18 U.S.C. §§ 1961(4) and 1962(c). The existence of this associated-in-fact enterprise is evidenced by Defendants' membership and communications in the Outsider Telegram channels, common use of Outsider, coordination in executing specific phishing attacks, and the commercialization of the attacks, which indicate that Defendants function similar to a black-market business enterprise. *See supra* ¶¶ 34–140.

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

Pattern of Racketeering Activity and RICO Predicate Acts

171. At all relevant times, Defendants have conducted or participated in, directly or indirectly, the conduct, management, and/or operation of the Outsider Schemes 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.

172. 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 a RICO predicate act under 18 U.S.C. § 1961(1). These activities have affected and continue to affect interstate or foreign commerce.

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

174. 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 their fraudulent schemes. Defendants have violated and continue to violate the wire fraud statute.

175. Defendants commit wire fraud in violation of 18 U.S.C. § 1343 each time they send text messages containing links to websites falsely purporting to be wireless service providers, government agencies, brokerage firms, and other legitimate entities or institutions to trick their victims into disclosing sensitive personal and/or financial information. In just a two-week period from May 18 to June 1, 2026, Google received more than 55,000 reports—including from users in the United States—of suspicious messages transmitted over Google Messages, including reports

of fraudulent phishing messages received from the Outsider Enterprise attempting to lure them into clicking links to fraudulent websites. For example:

a. On June 1, 2026, a U.S-based Google Messages user reported receiving a phishing message from Defendants that stated, "Your … account currently holds 18,400 points, scheduled to expire on May 26, 2026. Per the program terms, unused points will be removed automatically after this date and cannot be reinstated," followed by a link to a website domain created through Outsider to spoof the website of a U.S.-based wireless service provider.

b. On May 31, 2026, a U.S.-based Google Messages user reported receiving a phishing message from Defendants that stated, "Your vehicle registration renewal is suspended due to unpaid tolls. Use this official link to pay," followed by a link to a website domain created through Outsider to spoof the website of a Michigan state agency.

c. On May 26, 2026, a U.S.-based Google Messages user reported receiving a phishing message from Defendants that stated, "We've noticed you've accumulated a significant number of reward points in your … Rewards account. Please be sure to check the expiry date of your points to avoid them expiring," followed by a link to a website domain created through Outsider to spoof the website of a U.S.-based wireless service provider.

d. On May 28, 2026, a U.S-based Google Messages user reported receiving a phishing message from Defendants that stated, "We attempted to deliver your package on May 19, but were unable to complete the delivery. A signature was required at the time of delivery, and no one was available to sign for the item at the address on file.

To avoid any further delays, please select one of the following options," followed by a link created through Outsider to spoof the website of USPS.

e. On May 20, 2026, a U.S.-based Google Messages user reported receiving a phishing message from Defendants that stated, "We encourage you to take advantage of these rewards before time runs out. … This is a friendly reminder that your 11,430 … reward points will expire on December 24, 2029[.] As stated in our terms, any unused points will automatically be withdrawn after this date," followed by a link to a website domain created through Outsider to spoof the website of a U.S.-based wireless service provider.

176. 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 from being perpetrated on its customers and through its services.

Conspiracy to Violate RICO

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

178. 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).

179. 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. Indeed, Defendants discuss their criminal conduct openly as part of the conduct of the Enterprise. 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).

180. Defendants agreed to direct or participate in, directly or indirectly, the conduct, management, or operation of the Outsider 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 Outsider Enterprise's affairs. The purpose of the conspiracy was to commit a pattern of racketeering activity in the conduct of the affairs of the Outsider Schemes, including the acts of racketeering set forth above and the sale and use of Outsider to commit crimes, all for the purpose of enriching the Enterprise.

181. 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.

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

183. 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)

184. Google incorporates the foregoing paragraphs (¶¶ 1–183) of the Complaint as if set forth in full.

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

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

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

188. Defendants use 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)

189. 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' criminal 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.

190. 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.

191. 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)

192. 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.

193. 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).

194. 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)

195. 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).

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

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

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

199. 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.

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

201. 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).

202. 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.

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

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 Act and RICO;

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 as the Court deems just and reasonable.

Dated: June 12, 2026

Respectfully submitted,

/s/ Laura Harris

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

Benjamin S. Softness
KING & SPALDING LLP
50 California Street, Suite 3300
San Francisco, CA 94111-4624
Tel: (415) 318-1251
Fax: (415) 318-1300
bsoftness@kslaw.com

Counsel for Plaintiff Google LLC