UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

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

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

I, [redacted], declare as follows:

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

2. As a CCIG Investigator, I evaluate cybersecurity threats that target—or are discovered by cybercriminals' use of—Google products and services, including Android, Chrome, Gemini, Google Search, YouTube, Google Cloud, Google Drive, Google Play, and Google Pay. As part of a broader Google effort, my team works to investigate cybersecurity threats and identify and attribute attacks to protect Google users, products, services, platforms, and assets from serious cyber threats, including phishing attacks.[1] [redacted] While at Google, I have participated in and directed numerous phishing investigations and operations to disrupt internet infrastructure used by cybercriminals.

3. Google has investigated a group of cybercriminals who develop, maintain, and use an end-to-end software platform called "Outsider" to perpetrate widespread phishing scams. We refer to this group of cybercriminals as the "Outsider Enterprise" or the "Enterprise."

4. CCIG, working with other relevant Google teams, has assessed this Enterprise's activities and the impact they have had on Google and users of Google products. The conclusions in this declaration are based on Google's investigation. As part of that investigation, we have

[1] Phishing is a cybercrime in which attackers impersonate legitimate entities to trick people into clicking on a link or navigating to a website built to steal sensitive personal information.

concluded that the Enterprise's use of Outsider has caused significant harm to Google, its customers, and victims of Outsider phishing attacks. Outsider is a powerful software that can be used to spoof (*i.e.*, impersonate) legitimate websites and trick phishing victims into disclosing personal and financial information to members of the Enterprise. Outsider's impact has also been amplified by the use of artificial intelligence ("AI")—including Google AI tools—which the Enterprise encourages and enables. Outsider has facilitated, and continues to facilitate, the exponential growth of phishing attacks worldwide and in the United States. It will continue to cause serious harm if it persists unimpeded.

I. Google Products and Background

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

6. Google's search engine, accessible at www.google.com, is the most widely used internet search service in the world. Gmail is a free email service used by more than 1.5 billion people worldwide that integrates Google Search and offers freedom from pop-up or irrelevant advertising. YouTube is an online video-sharing platform on which users watch more than one billion hours of content every day.

7. Gemini is Google's family of large language AI models and the chatbot interfaces for interacting with those models. The Gemini chatbot ("Gemini") allows users to submit requests using plain-language prompts and generate text, images, or even computer code. Gemini can help users with a range of practical, time-saving tasks. It can share a user's camera or screen to provide real-time assistance—for example, giving live step-by-step guidance about how to fix a printer, and it can perform time-consuming web browsing to compare hotel prices and complete bookings. It can offer advice in plain language, create a visual mock-up of a new haircut using a photo of the user, and it can write and debug software code.

8. Google maintains its position as a leader of multiple sectors through a sustained commitment to offering products that are both dependable and advanced, including ensuring that Google products are secure by default. Google has pioneered technologies used by millions of people, including the following products or services:

a. **Android**: Android is an operating system 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 Declaration, where I refer to "Android," I am referring 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 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 safe. 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. **Google Search Console**: Google Search Console is a product that provides tools to measure a website's search traffic and performance.

l. **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.

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

9. Each of these products and services, in addition to others, contributes to the value of Google's brand, which is one of the most prominent and valuable brands in the world. Google has achieved this level of brand recognition over the course of nearly three decades by focusing on delivering safe and quality products. Google also expends significant resources to maintain the quality of its brand, including by providing extensive guidelines governing the use of Google trademarks (also referred to as Google's "Marks") to ensure those trademarks are used to promote and not diminish Google's reputation and to preserve Google's position as one of the world's most trusted technology brands.

II. Google's Commitment to Cybersecurity

10. For the past two decades, Google has made security the cornerstone of its business. Our commitment to security begins with our product strategy. The company does not simply respond to security incidents or plug security holes. Instead, Google works to eliminate entire

classes of threats for users and businesses who depend on our services. It strives to keep users safe by making our products secure by default—by using progressive layers of both digital and physical protection to block malware and cyberattacks, and by employing the best engineers in the world.

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

12. Google allocates substantial resources to detecting and restricting phishing communications and protecting users when they use Google products. These efforts include, among other things, developing and constantly improving spam filters, flagging suspicious communications for the user, incorporating two-step verification protections, publicly reporting known phishing websites, scanning email attachments, and detecting and preventing suspicious account sign-ins.

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

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

15. Google's security efforts also extend to AI. With respect to Gemini specifically, Google imposes content filters that operate independently from the model itself. These filters prevent the model from producing certain categories of content, such as sexually explicit or dangerous content. When users ask the model to produce prohibited content, those requests trigger Gemini's safety systems and the content is not generated.

16. Google also has security systems in place to detect more malicious uses of its AI tools, such as the creation of malware for the furtherance of cybercrime, including where users have relied on Gemini to assist with coding malicious software, generating malicious promotional content, and engaging in language-to-language translation to further their malicious aims. When this activity is detected, Google investigates and takes corrective action, including disabling offending accounts when necessary, and uses its findings to strengthen Gemini's safety systems.

17. In addition to automated triggers, Google's Trust & Safety, threat-intelligence, and security teams work jointly to address and adjust to real-world misuse. When Google identifies actors attempting to exploit Gemini in ways that may not be caught by existing security measures,

it takes corrective action, including disabling their accounts and associated projects, and immediately incorporates intelligence from those incidents to improve Gemini's defenses.

18. Recently, Google has shut down the harmful misuse of Gemini by foreign actors. In one instance, China-based cybercriminals posing as participants in a cybersecurity exercise tried to use Gemini to find weaknesses in computer systems, craft convincing fake messages to trick targets into revealing sensitive information, and develop tools to secretly extract data from compromised networks. In a separate campaign, Iranian state-sponsored actors pretended to be students working on a university project but were actually seeking to develop malware. They asked Gemini to help develop that malware, including tools that would let the group remotely control compromised web servers. In another campaign, North Korean actors used Gemini to research cryptocurrency theft techniques, develop code to steal from crypto wallets, and craft fake software update instructions to extract user credentials from owners of cryptocurrency. In each case, Google blocked the accounts and strengthened its underlying protective systems based on the insights it gleaned.

19. Google uses what it learns from real-world misuse to strengthen not only the filtering and security mechanisms that sit on top of Gemini, but also to refine the model itself, which, over time, is trained to recognize and refuse similar attempts in the future. Moreover, Google continuously strengthens these protections through "automated red teaming" ("ART"), a process in which internal security teams simulate realistic attacks to identify vulnerabilities before product release. When ART uncovers weaknesses, Google conducts "model hardening," which trains Gemini on large sets of malicious-input scenarios so that the model can recognize and disregard embedded malicious instructions.

20. As an additional line of defense, Google empowers users to detect potential fraud by applying a durable watermark to Gemini's text and image outputs. This gives users the ability to immediately identify AI-generated content and to apply any due scrutiny.

21. CCIG's work has been essential to disrupting numerous major cybersecurity threats, including significant botnet[2] threats such as Glupteba,[3] Cryptbot,[4] BadBox, and BadBox 2.0,[5] and phishing threats like Lighthouse,[6] Darcula,[7] and now Outsider.

III. Phishing-as-a-Service and Outsider

22. With other Google investigators, I investigate cybercrime campaigns that are perpetrated using the phishing-as-a-service ("PhaaS") model and that target Google and its customers. In this role, I have investigated the Outsider Enterprise and its PhaaS campaign.

23. Phishing is a type of cyberattack in which cybercriminals send emails, text messages, or electronic messages that impersonate legitimate organizations—such as brokerage firms or telecommunications companies—to lure the recipient victims into visiting a malicious website disguised as that organization's website. The impersonations often include the use of Google's name, brands, or logos. Once on the familiar-looking site, victims are tricked (for example, by being asked to "log in") into disclosing sensitive information like passwords, credit

[2] A botnet is a network of internet-connected devices that has been infected with malware and is controlled by cybercriminals.
[3] Royal Hansen & Halimah DeLaine Prado, *New action to combat cyber crime*, Blog.Google (Dec. 7, 2021), https://tinyurl.com/bde3v5fy.
[4] Mike Trinh & Pierre-Marc Bureau, *Continuing our work to hold cybercriminal ecosystems accountable*, Blog.Google (Apr. 26, 2023), https://tinyurl.com/pktmdsrc.
[5] Google, *We're taking legal action against the BadBox 2.0 botnet.*, Blog.Google (July 17, 2025), https://tinyurl.com/yc7jw5fm.
[6] Halimah DeLaine Prado, *A dual strategy: legal action and new legislation to fight scammers*, Blog.Google (Nov. 12, 2025), https://tinyurl.com/ycxbub5n.
[7] Kevin Collier, *Google sues alleged Chinese scam group behind massive U.S. text message phishing ring*, NBC (Dec. 17, 2025), https://tinyurl.com/47jxfxr3.

card numbers, or banking information. PhaaS turns this criminal activity into a business model. Cybercriminals develop, maintain, and sell software and support services that facilitate phishing schemes for criminals who may lack the technical know-how to execute such a scam. This software, also sometimes referred to as a "phishing kit," provides the infrastructure necessary to create a fake website (or other platform) and collect and store stolen personal and/or financial information. A typical phishing kit may include fake website templates and training videos on how to use the phishing software, making it relatively easy for those without technical expertise to create a phishing campaign. These kits rely on a variety of respected brands—including Google—to lure targets into believing they are interacting with a legitimate entity and trick victims into sharing sensitive personal and financial information with untrustworthy sources.

24. Phishing kits, like Outsider, make cybercrime easier for less technically skilled perpetrators because they supply a user-friendly interface—and access to a network of other variously skilled criminals—to help complete otherwise technical tasks (such as designing a fake website with fake payment pages). Additionally, these kits make cybercrime significantly cheaper and less resource-intensive because cybercriminals do not need to expend significant financial resources to develop and scale their infrastructure. With a phishing kit, the marginal work required to create multiple sites mimicking multiple brands is close to trivial. The PhaaS model is therefore lucrative because it enables widespread and fast-paced phishing activities.

25. The black market for PhaaS is competitive. Our investigation has observed Outsider's developers "hardening" (or securing) their software against detection and attack. We understand these steps to be aimed not only at evading legal authorities and industry defenses, but also at guarding against theft by other cybercriminals seeking to steal (rather than license) Outsider code to use for their own scams—what in a legitimate market, would be intellectual property theft.

26. Outsider is a phishing kit software sold by the Outsider Enterprise. Its users can create, design, and customize phishing sites with ease—including by adding Google logos and replicating fake versions of Google Pay's payment pages. Once a phishing page is complete, the Enterprise distributes links to the phishing websites through iMessages, RCS messages, and SMS messages. Outsider end-users can then monitor their attacks directly from a dashboard on Outsider's homepage. As victims type their personal and/or financial information into the fraudulent website, the Outsider software collects the information and sends it directly to the Enterprise in real time. It can even automatically create digital cards with the victims' payment information.

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

IV. Google's Investigation into the Enterprise

28. As part of its investigation into the Outsider Enterprise, Google has identified both Google accounts and malicious phishing domains associated with Outsider.

29. Google has discovered a series of Google accounts tied to the online persona "Chenlun," whom we believe to be a member or members of the Outsider Enterprise. Chenlun could be a person, a collection of persons, or an entity using that name in various ways on the internet. Through the investigative steps described below, my team traced the Chenlun persona across multiple Google accounts, Google Cloud infrastructure, and Telegram channels. Using that information, Google was able to establish Chenlun's connection to the development and distribution of the Outsider phishing software.

30. The Chenlun persona was first observed operating a PhaaS service in fall 2022. Following an article published by cybersecurity researchers in October 2023 that publicly identified the operation, the actor behind the Chenlun persona went dark.[8] The same actor reemerged in May 2025 under the alias "sinkinto01" and began marketing Outsider—the current version of the phishing software.

31. The Outsider Enterprise uses Telegram channels to communicate regarding the Outsider software and to distribute videos instructing users on how to use various features of the software to design and execute phishing attacks. One such video helped Google track Outsider to the Chenlun persona.

32. On August 2, 2025, a threat actor posted a tutorial video to the Telegram channel https://t[.]me/sinkintopd demonstrating the Outsider software's ability to automatically back up stolen data to Google Drive. The video's description, written in Chinese,[9] stated: "#Automatic Cloud Backup / Mom no longer worries about me losing my fish"—"fish" meaning phishing victims. In the course of demonstrating this Google Drive backup functionality, the actor exposed a Google account on screen: [redacted]

33. On the same day, the same threat actor posted a second tutorial video to the same Telegram channel demonstrating the ability to use Google's Gemini AI tool to write code for custom phishing pages in minutes. The video's description, also written in Chinese, stated: "#Customization Features, Part 2 #Core / Full customization capabilities: Create custom component pages from scratch using AI. A must-read for advanced customization."

[8] *See* Brian Krebs, *Phishers Spoof USPS, 12 Other Natl' Postal Services*, Krebs on Security (Oct. 9, 2023), https://tinyurl.com/37nf7eyd.
[9] My team used Google Translate to translate posts that were originally in Chinese to English. The quoted language of posts in this Declaration reflects those translations.

34. As of the date of this declaration, both tutorial videos remain live on the Telegram channel. Because the actor posting these videos had access to the [redacted] Google account and was demonstrating the Outsider software's core functionality, my team concluded that this account is operated by the actor behind the Chenlun persona.

35. Google's investigation further identified multiple overlapping account attributes linking additional email addresses—[redacted] and [redacted]—to the Chenlun persona.

36. My team's investigation also revealed connections between both the [redacted] and [redacted] accounts and the Outsider infrastructure. Based on our investigation, we concluded that the [redacted] the functionality of the prior version of the Outsider phishing kit.

37. While these accounts do not contain any billing information or an identifiable name, the accounts have consistent login activity geolocating to Hong Kong. In my experience, cybercriminals often use internet proxy services, which obscures their real locations, making it impossible to know where the users of these accounts are actually located. The activity on the accounts described above shows signs of the use of proxies. That means that my team cannot pinpoint the users' locations. It is also suspicious because my experience has taught me that cybercriminals often use these proxies to help them evade detection.

38. My team has also worked to identify malicious phishing domains associated with the Outsider software. [redacted]

[redacted] In particular, Google analysts [redacted] Google analysts also [redacted] Google analysts [redacted] That search generated a list of domains that we concluded were created with the Outsider software. Google provided the search results to NAXO to independently verify that the domains are malicious phishing sites.

V. The Outsider Enterprise's Use of Google Products

39. The Outsider Enterprise exploits free Google tools to carry out phishing schemes in violation of many of Google's policies. For example, the Outsider Enterprise uses victims' stolen credit card information by adding those stolen credit cards to Google Wallets on Android devices.

How the Outsider Enterprise Uses Google Messaging Services

40. The Outsider Enterprise distributes phishing messages to potential victims on Android devices that receive Google Messages through the RCS messaging protocol.

41. Google's services offer users the ability to report suspected spam and other malicious messaging activity delivered via Google Messages. Google Messages contains spam protection identifying different types of spam, including phishing attempts. Spam detection works with message data on users' devices to detect spam and may also use those signals to train AI models to improve spam detection.

42. In the period between May 18 and June 1, 2026, Google received more than 55,000 reports of suspicious messages transmitted over Google Messages from users, including users in the United States, and 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.

43. According to my team's investigation, the Enterprise sent 2,628,368 messages to Android users containing links to Outsider-generated websites over this two-week period. In response to the phishing messages, Google has taken action to block further Google Messages containing Outsider-generated websites from being distributed to users.

44. The Outsider Enterprise's use of Google Messages violates Google's Terms of Service, which prohibit "accessing or using our services or content in fraudulent or deceptive ways, such as … phishing" or "creating fake accounts."[10] When accounts are identified as violating Google's terms in the manners described above, the accounts are closed.

How the Outsider Enterprise Uses Google's Cloud-Based Products

45. As another means of exploiting Google's products, the Enterprise uses Google's cloud-based services. For example, the Enterprise integrated Google Drive into the Outsider

[10] Google, *Terms of Service*, https://tinyurl.com/4f59tyr9 (last visited June 10, 2026).

software as a "backup feature," which enabled Enterprise members to export and store stolen personal and financial information directly to Google Drive. Google has since blocked Outsider's access to Google Drive by suspending the account supporting it. Enterprise members also procure Google Cloud servers to host phishing websites created by the Outsider software.

46. These abuses of Google Cloud violate 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."[11]

47. The Outsider Enterprise's abuses of Google Drive and Google Cloud also violate Google's Terms of Service, which prohibit "accessing or using our services or content in fraudulent or deceptive ways, such as … phishing" or "creating fake accounts."[12]

How the Outsider Enterprise Uses Gemini

48. In August 2025, the Outsider Enterprise created a tutorial video, distributed through its Telegram channel, that explains how Enterprise members can leverage AI to amplify Outsider's capabilities and accelerate the development of fake websites. In that video, the Outsider Enterprise used the Gemini chatbot interface (gemini.google.com/app) to showcase how Outsider could create, in a matter of minutes, a spoofed version of the web page that could facilitate a new phishing scheme.

49. This abuse of Google's Gemini tool enhances the Enterprise's ability to execute phishing schemes because it enables cybercriminals to create a limitless range of realistic-looking

[11] Google, *Google Cloud Acceptable Use Policy*, https://tinyurl.com/226jfyap (last visited June 10, 2026).
[12] Google, *Terms of Service*, https://tinyurl.com/4f59tyr9 (last visited June 10, 2026).

websites in minutes without any technical expertise. This use of Gemini 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."[13]

VI. The Outsider Enterprise's Use of Google Trademarks

50. The Enterprise uses Google's Marks in its pre-built phishing templates in addition to offering customization tools that allow users to add Google Marks to any page. Outsider provides more than 290 templates to create phishing websites that mimic legitimate websites of reputable organizations and businesses to encourage victims to enter their sensitive personal and financial information under false pretenses. Many of these phishing websites also feature Google's trademarks for products such as Google Pay, YouTube, or Google Play on the sign-in or payment screens.

51. For example, several pages mimicking government agencies, such as the District of Columbia Department of Motor Vehicles, the Minnesota Department of Public Safety, the Georgia Department of Driver Services, and the Florida Department of Highway Safety and Motor Vehicles, feature the YouTube logo. In the ordinary course, the presence of the YouTube logo indicates that the entity to whom the website belongs has a YouTube channel, and the icon acts as a link to that channel. A Google Play icon indicates the presence of an app for that entity in the Google Play app store, and acts as a link to the app store. Other Google logos indicate similar linkages to Google products. A USPS phishing template likewise displays a YouTube logo, as does a template mimicking a financial institution. A T-Mobile rewards phishing page template includes Google Play and YouTube logos, while a template mimicking the Qantas rewards portal includes a

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

YouTube logo. Shopify-based payment pages prominently feature the Google Pay logo. In the ordinary course, the presence of the Google Pay logo indicates that the entity to whom the website belongs accepts payment through Google Pay, a legitimate digital wallet and payment service operated by Google.

52. Beyond these pre-built templates, Outsider also provides tools allowing users to customize phishing pages by importing images, modifying page layouts, and adding branding elements—including Google logos.

53. A list of Google's Marks the Outsider Enterprise has used without Google's permission in its cybercrime activities is attached as **Appendix D**.

54. Outsider's use of these logos violates Google's guidelines for proper usage of its trademarks and brand features (defined as product names, logos, screenshots, and other distinctive features),[14] which forbids, among other things, "display[ing] a Google Brand Feature on a site that violates any law or regulation," "display[ing] a Google Brand Feature in any manner that implies a relationship or affiliation with … Google," and "display[ing] a Google Brand Feature in a manner that is…misleading[] [or] infringing."[15] There are further requirements for the use of certain Google logos and icons. For example, Google's brand team must "review[] and fully approve[]" any use of the Google Play trademark.[16]

55. Given Google's tenure as a trusted technology provider and its reputation for providing secure internet products, victims likely view the presence of a Google trademark as an

[14] Google, *Google Play: Legal and trademarks*, Partner Mktg. Hub, https://tinyurl.com/4vd29caf (last visited June 10, 2026).
[15] Google, *Trademark guidelines for proper usage*, Brand Res. Ctr., https://tinyurl.com/fppdbffw (last visited June 10, 2026).
[16] Google, *Google Play Legal Requirements*, Partner Mktg. Hub (last visited June 10, 2026), https://tinyurl.com/4vd29caf.

indicator that the website is safe or legitimate. The Outsider Enterprise is using Google's branding—and the goodwill associated with it—to convince victims to turn over their sensitive financial data.

VII. The Outsider Schemes Are Causing Harm to Google, Its Users, and the Public

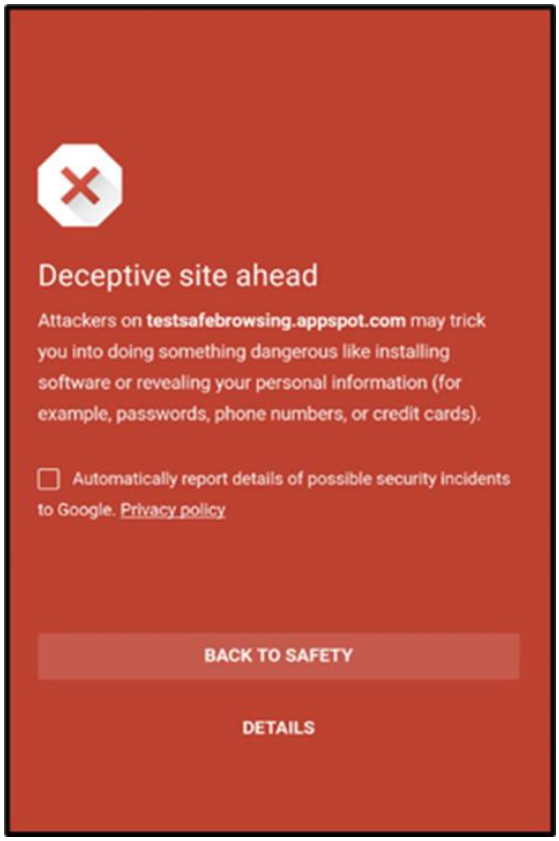
56. The Outsider Enterprise's criminal actions have affected Google, its users, and the public. It is estimated that there have been well over 100,000 victims of the Enterprise.

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

58. Google has devoted (and continues to devote) substantial resources to detect, deter, and disrupt the Enterprise's activities, including fraud-protection activities like flagging malicious websites and Google Messages sent through RCS, and suspending the accounts supporting the software's Google Drive feature and the Enterprise's Google Cloud use.

59. Between November 14, 2025, and April 14, 2026, alone, Google detected over 1.59 million phishing webpages linked to the Outsider Enterprise, with tens of thousands of new webpages appearing daily and 62,993 appearing in a single day at peak activity. In response to this phishing activity, Google implemented the Safe Browsing feature to warn Google Chrome users who attempted to access Outsider phishing webpages. Upon the Safe Browsing warning going live, an example of which is pictured below, there was a dramatic decrease in traffic to Outsider phishing webpages on the Google Chrome browser. Individuals using other web browsers may not

see such a warning upon clicking on Outsider phishing webpages. Google takes these steps because Outsider poses a threat to Google's brand and reputation, as well as to Google's users.



60. As Google and other cybersecurity actors respond to the Enterprise's phishing websites, the Enterprise continues to shift and generate new webpages. The Enterprise's constant adaptation and Google's continued cybersecurity efforts contribute to the significant volume of domains that are being generated daily.

61. Google has spent hundreds of hours investigating and remediating Defendants' activities. Google will be forced to continue these efforts for as long as the Outsider Enterprise's activities continue. The cost of investigating the Outsider Enterprise, assessing the damage it causes, and determining whether any remedial measures are needed has been significant.

62. Despite Google's best efforts, the Outsider Enterprise's cybercrime continues to pose an imminent and irreparable injury to Google's business and reputation.

63. Beyond Google, the continued proliferation of phishing, smishing, and PhaaS is a threat to Google's users and the public as a whole.

64. In my experience, cyberthreat detection work is best done in secret. Due to its sophisticated nature, I believe that if the Outsider Enterprise were given advance notice that the website domains and IP addresses it uses in its phishing operation would be disabled, the Enterprise would take measures to frustrate any disruption efforts in order to preserve the phishing operation.

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

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

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

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

d. Take these steps without advance notice to the Enterprise.

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

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

In accordance with 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct. Executed on 6/10/26, in [redacted]