UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC, *Plaintiff,* v. DOE 1 a/k/a YUCHENG CHANG and DOES 2–25, *Defendants.*	Civil Action No.:

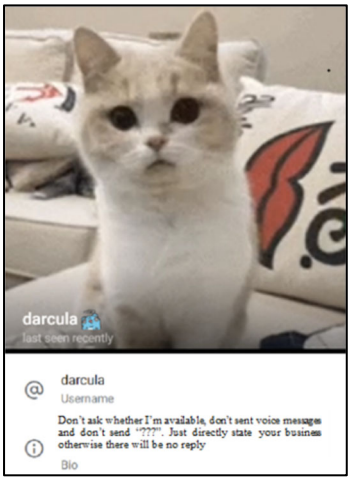
COMPLAINT FOR DAMAGES AND INJUNCTIVE RELIEF

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

INTRODUCTION

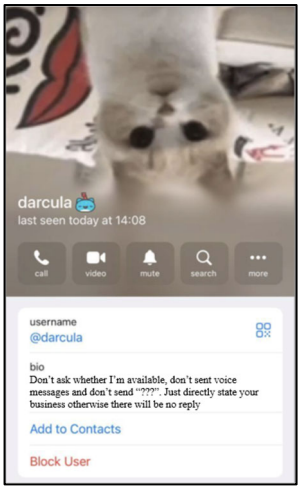
1. Defendants are a group of foreign cybercriminals who design and execute novel "phishing" attacks,[1] using artificial intelligence ("AI") technology to mimic legitimate websites and dupe victims into disclosing personal and financial information. These attacks have swindled millions of victims globally, including Google customers, and have exploited Google's reputation through the unauthorized use of its trademarks and impersonation of Google's services. To combat these cybercrimes, Google is seeking an injunction to disrupt Defendants' criminal enterprise and the infrastructure on which it relies.

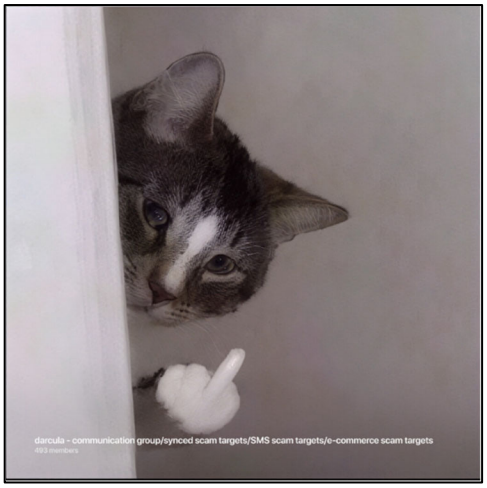
2. In 2023, Defendants developed and deployed an end-to-end phishing software known as "Magic Cat," a "phishing for dummies" kit that provides the technical infrastructure to create and deploy large-scale phishing attacks for those with little technical know-how. Operating online under the alias "Darcula," Defendants are known for their signature use of cat images as profile pictures.[2]



[1] A "phishing" attack is a form of cyberattack that dupes victims into clicking on malicious links with false messages, such as purported notices about a lost package or unpaid toll.

[2] Erlend Leiknes & Harrison Sand, *Exposing Darcula: a rare look behind the scenes of a global Phishing-as-a-Service operation*, Mnemonic (May 4, 2025), https://tinyurl.com/537tm5bs.





3. Magic Cat's developers and their network of collaborators and co-conspirators—including those who deploy Magic Cat to execute phishing campaigns—are referred to herein as the "Darcula Enterprise" or the "Enterprise."

4. Magic Cat is not simply a back-end technical tool; the software provides a suite of easy-to-use resources to create, deploy, and monitor criminal phishing campaigns on a user-friendly interface. The latest version of the software features cutting-edge AI technology capable of creating a fake version of any website in minutes, tools to bring the websites online, administrative functionality to track and store stolen data, and advanced troubleshooting and customer support features, all designed and maintained to evade detection and lead victims to believe they are transacting with legitimate businesses and government entities.

5. Using Magic Cat, Enterprise members create phishing campaigns and send mass text messages to potential victims—for example, luring them to sign up for what purports to be (but is not) a free trial of Google's YouTube Premium service through a spoofed version of Google's YouTube Premium sign-up webpage, or warning them (falsely) that their bank account is compromised. Those fake websites are nearly indistinguishable from the real thing and often bear the hallmarks of legitimate sites, even purporting to permit victims to sign in through a Google

account, and tricking victims into turning over their personal information, credit card numbers, and other sensitive financial data, which the Darcula Enterprise uses to steal victims' money or sells to other criminal actors.

6. At its height, researchers estimated that the Enterprise was responsible for upwards of 70 to 80% of all phishing text messages, with at least 600 cybercriminals coordinating to deploy and execute its phishing schemes to unsuspecting victims across the globe.[3] Over the course of just seven months, the Darcula Enterprise stole nearly 900,000 credit card numbers from individuals around the world, including nearly 40,000 credit card numbers from individuals in the United States alone.

7. Today, thanks to the work of the cybersecurity experts and journalists who have alerted the public to the Darcula scheme,[4] the Enterprise has reduced its profile and no longer openly markets its software. But Google's investigation has revealed that new Magic Cat-linked phishing websites continue to be created daily and that significant portions of the Enterprise's cyber infrastructure remain in place, ready to be redeployed at any moment.

8. The Enterprise preys upon the public's trust in Google, a leader in the technology space, by misappropriating Google branding, including by incorporating Google's trademarks (as further defined herein, Google's "Marks") into fraudulent websites including by impersonating Google's YouTube platform. The Enterprise interferes with Google's relationships with its users (and potential users), harms Google's reputation, impairs the value of Google's products and services, and forces Google to devote substantial resources to investigate and combat the Enterprise's criminal activity, causing Google financial harm and undermining customer goodwill.

[3] Martin Gundersen, *Inside the Scam Network*, NRK (May 4, 2025), https://tinyurl.com/5n6cp2jd.
[4] *See id.*

9. Google therefore brings this action under the Racketeer Influenced and Corrupt Organizations Act ("RICO"), the Lanham Act, and the Computer Fraud and Abuse Act ("CFAA") against Defendants to disrupt their criminal enterprise and prevent it from causing further harm, and to recover damages.

PARTIES

Plaintiff

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

11. Google is a leading technology company that offers a wide variety of services to organize the world's information and make it universally accessible and useful. Its search engine, accessible at www.google.com, is the most widely used internet search service in the world. Gmail, a free email service used by more than 1.5 billion people worldwide, includes a variety of revolutionary and innovative features, including an industry-leading two full gigabytes of email storage; email message threading; fast, precise search of emails using an integrated Google search engine; and freedom from pop-up or irrelevant advertising. Google also offers YouTube, an online video sharing platform that millions of people use to share and watch videos each day. While YouTube is a free platform, Google also offers a premium version of YouTube on a subscription model through which subscribers can access YouTube with no advertisements, download YouTube videos for offline viewing, and watch YouTube videos "in the background"—in other words, while using other applications on mobile devices.

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

a. **Android**: Android is an operating system created by Google that is designed to run on mobile devices, such as smartphones or tablets. Google has both a proprietary

version that is used for official 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 created and operated by Google that runs on various operating systems, including on personal computers, smartphones, and tablets.

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

d. **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.

e. **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.

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

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

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

h. **YouTube**: YouTube is an online video sharing platform. YouTube Premium provides premium, ad-free access to YouTube content with a subscription and can be purchased online.

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

Defendants

14. Defendant Doe 1 a/k/a Yucheng Chang is an individual who has conspired with other Defendants to engage in a pattern of racketeering activity. He has played a significant role in the development and maintenance of Magic Cat, participated in the management and operation of the Darcula Enterprise's phishing schemes, and committed criminal acts that have caused harm to Google, its users, and numerous others, as described below. He resides in China.

15. Defendants Does 2–25 are other individuals or entities who have conspired to engage in a pattern of racketeering activity. They have each participated in the operation or management of the Darcula scheme and engaged in criminal acts that have caused harm to Google, its users, and countless others. Defendants reside in China or other foreign countries.

16. At this time, Google does not know the true names and capacities of the Doe Defendants. Each of these Defendants is responsible in some manner for the conduct alleged, having agreed to become part of the Darcula Enterprise.

17. Google is presently aware of multiple connected Doe actors within the Darcula Enterprise. It is not clear precisely how many actors or groups comprise the Enterprise; the Doe numbers are meant to be representative. All the threat actors are connected to one another through overlapping infrastructure and historical and current business ties. The threat actors' misconduct is described in more detail below.

JURISDICTION AND VENUE

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

19. Defendants are subject to personal jurisdiction in this district, and the exercise of jurisdiction over Defendants is proper pursuant to 15 U.S.C. § 1121; 18 U.S.C. § 1965; and N.Y. C.P.L.R. §§ 301 and 302. Defendants have transacted business and engaged in unlawful and 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 used Google logos as part of spoofed websites 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 conspiracy and fraud. Defendants were aware of the effects in the United States and New York of those acts; the activities of their co-conspirators and agents were to the benefit of Defendants; and their co-conspirators and agents were working at the direction, under the control, at the request, and/or on behalf of Defendants in committing those acts.

20. Defendants have affirmatively directed actions at the United States, including the Southern District of New York, by attempting to and successfully phishing personal financial information from hundreds of victims in New York, including at least one hundred victims in the Southern District of New York. Defendants have aimed each of these illegal activities at individuals within the Southern District of New York.

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

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

FACTUAL ALLEGATIONS

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

23. As personal devices and email have replaced telephone lines and traditional mail, criminal activity has likewise evolved and is leveraging those tools to reach more victims with less effort. One of the most common forms of internet-based criminal schemes is phishing. The sophistication and reach of phishing schemes have grown dramatically—cybercriminals are now

sending an estimated 3.4 billion phishing emails every day.[5] Phishing has become the most ubiquitous form of criminal fraud.

24. "Phishing" is a type of cyberattack in which threat actors impersonate well-known brands, government agencies, or known individuals within an organization to trick individuals into disclosing their sensitive information, like passwords, credit card numbers, or banking information. The attacker sends victims a deceptive message in an email or other electronic communication that is crafted to appear trustworthy. The phishing message asks the target to click a link or fill out a form to transmit their personal data, which threat actors then steal for their own criminal use.

25. "Smishing" is a type of phishing where threat actors use text messages (such as SMS or RCS messages) to trick victims into turning over their information. The threat actors often use urgent language to cause the recipient to fear that if they do not act immediately to remediate the (fake) issue, there will be consequences. These messages, which target thousands of phone numbers at a time, encourage recipients to click on a malicious link that leads to a fraudulent phishing website.

26. Smishing is especially nefarious because victims tend to "place more trust in these types of messages than in email."[6] That trust, paired with the heightened sense of urgency conveyed by these messages, "results in a significantly higher expected conversion rate than email … and other techniques the actors could use."[7]

---

[5] Sienna Arellano & Ian Kilty, *The Phishing Business Model*, Colo. State Univ. System: Info. Tech. (Feb. 17, 2025), https://tinyurl.com/psxum3se.
[6] Resecurity, *Smishing Triad Is Now Targeting Toll Payment Services in a Massive Fraud Campaign Expansion* (Apr. 8, 2025), https://tinyurl.com/8jsb3dm7.
[7] *Id.*

27. Once threat actors have sensitive information in hand, they can use it to access victims' email accounts, bank accounts, and more. Scammers often load the stolen payment cards to digital wallets—like Google Wallet—on mobile devices and then sell the mobile devices to others. Scammers can also relay new stolen card information in real time to devices used by co-conspirators to make in-person purchases, a practice known as "ghost tapping."[8] Some recent law enforcement actions have identified criminal networks using phones loaded with stolen credit card information and tap-to-pay functionality to purchase gift cards in bulk.[9] Other groups simply purchase their own tap-to-pay machines and configure them to deposit payments into their own bank accounts, using customer cards to make payments directly to themselves.[10] Still others use stolen brokerage firm credentials to perpetrate a modern iteration of a "pump and dump" scheme, pre-purchasing shares of a particular stock and then using compromised brokerage accounts to purchase large volumes of the stock, inflating the price before they liquidate their original holdings.[11]

28. These schemes have proven to be enormously profitable, meaning that the infrastructure necessary to execute them has become a commodity as well. So-called phishing-as-a-service ("PhaaS") is a business model that distributes software and support services to facilitate phishing, making it relatively easy for those without technical expertise to create and execute a

[8] Insikt Group, *Ghost-Tapping and the Chinese Cybercriminal Retail Fraud Ecosystem*, Recorded Future (Aug. 14, 2025), https://tinyurl.com/4fb77c7e.
[9] Josh Jarnagin, *Knox County Detectives Investigating 'Ghost Tap' Credit Card Fraud*, WVLT8 (May 31, 2025), https://tinyurl.com/bdffxm4y; *see also* Singapore Police Force, *Unauthorised Card Transactions Made Using Contactless Payment Methods in Singapore* (Feb. 17, 2025), https://tinyurl.com/mwx6nv76.
[10] *See* Brian Krebs, *How Phished Data Turns into Apple & Google Wallets*, KrebsOnSecurity (Feb. 18, 2025), https://tinyurl.com/37a3fzps.
[11] *See* Brian Krebs, *Mobile Phishers Target Brokerage Accounts in 'Ramp and Dump' Cashout Scheme*, KrebsOnSecurity (Aug. 15, 2025), https://tinyurl.com/4mv37y8b.

phishing campaign. The software, sometimes referred to as a "phishing kit," provides the infrastructure necessary to create fake websites (or other platforms), send bulk text messages or emails to victims, and collect and store stolen personal and financial information. For example, a phishing kit may contain ready-made website templates that closely resemble legitimate websites. Phishing kits enable criminals without technical expertise to engage in phishing and smishing, to reach larger numbers of targets, and to mimic a greater number of websites, making these types of attacks much more frequent and effective.

29. The PhaaS model also makes stopping phishing attacks more difficult. "Catching the person who carried out the attack does not put an end to the story. You will still have to catch the guy who designed the phishing kit and the one who provided it."[12]

The Magic Cat Phishing Software

30. First identified in July 2023,[13] Magic Cat is a bundle of software tools that enables threat actors to create spoofed text messages and websites through which unsuspecting victims—who believe the text or website is legitimate—disclose their personal and financial information. Magic Cat includes templates of fraudulent phishing websites that are designed to resemble legitimate websites.

31. The Magic Cat software package[14] includes two integrated components: (1) front-end software that is used to create, design, and edit phishing websites, and to configure

[12] Andreea Chebac, *What Is Phishing-as-a-Service (PhaaS) and How to Protect Against It*, Heimdal (July 7, 2025), https://tinyurl.com/5n6mp39p.
[13] Jessica Lyons, *Darcula adds AI to its DIY phishing kits to help would-be vampires bleed victims dry*, The Register (Apr. 25, 2025), https://tinyurl.com/ywban2f6; Ravie Lakshmanan, *Darcula Phishing Network Leveraging RCS and iMessage to Evade Detection*, The Hacker News (Mar. 28, 2024), https://tinyurl.com/2s4fhcnj.
[14] This software is sometimes referred to as "Darcula" software; however, users typically refer to the entire software package as "Magic Cat," the term used to refer to the software herein.

certain aspects of the phishing kit; and (2) a server-based program that is used to deploy phishing sites and collect stolen information from victims who are tricked into entering credit card information.

32. Much like legitimate software, Magic Cat is designed for ease of use. From the Magic Cat platform, a threat actor can generate a spoofed website and phishing "bait" messages, launch their phishing campaign, collect personal and financial data submitted by phishing victims, transform stolen financial information into virtual credit cards for immediate criminal use, and even monitor the relative success of their schemes through a sleek performance dashboard.

33. The earliest versions of Magic Cat offered around 200 phishing templates that spoof the websites of well-known brands in over 100 countries.[15] At the height of its use, it featured more than 300 templates.[16] Many of Magic Cat's templates are designed to target U.S. victims, such as websites spoofing the webpages of the Internal Revenue Service and the U.S. Postal Service ("USPS").

34. Members of the Enterprise distribute Magic Cat via several Telegram channels,[17] including the @darcula_channel, and on various sites on the dark web.

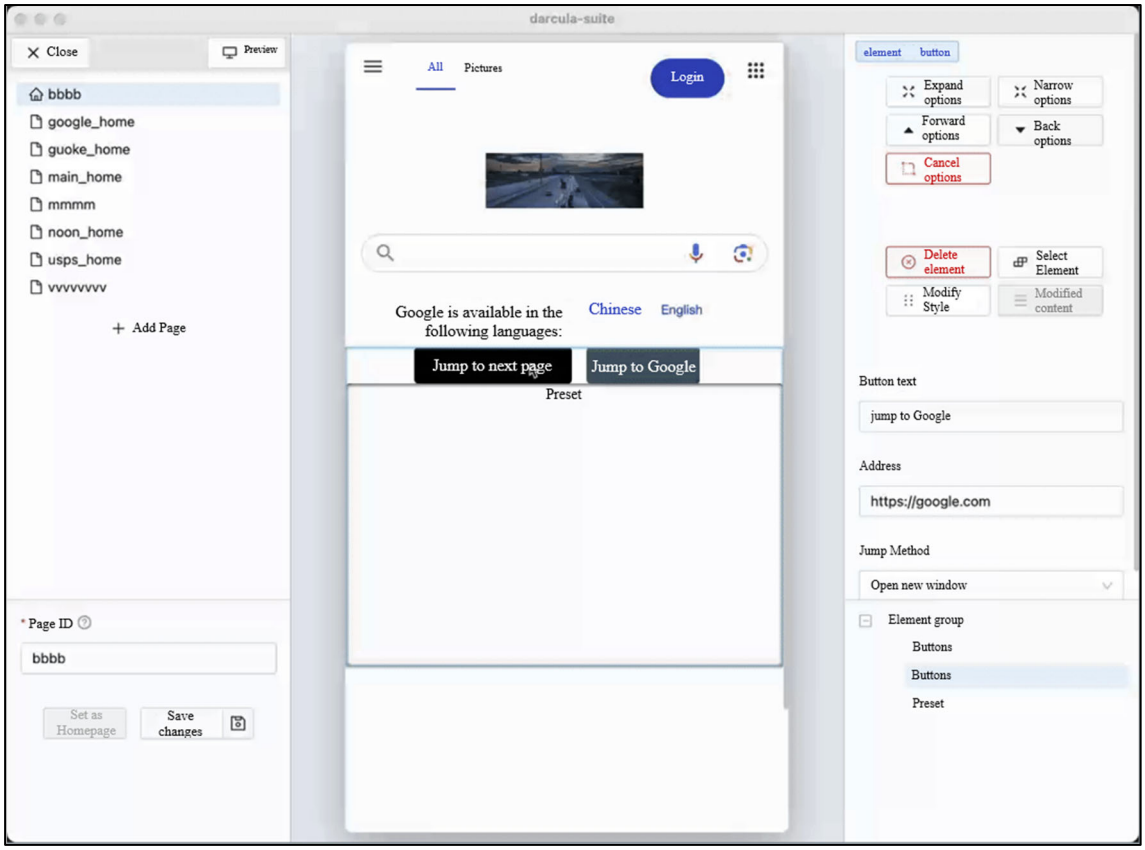
35. Earlier this year, the Darcula Enterprise debuted an even more pernicious version of the Magic Cat software. This latest iteration integrates generative AI and other features that allow the Enterprise to create near-perfect duplicates of virtually any legitimate website in minutes, without any programming knowledge. Members of the Enterprise simply input the URL of a

[15] Ravie Lakshmanan, *Darcula Phishing Network Leveraging RCS and iMessage to Evade Detection*, The Hacker News (Mar. 28, 2024), https://tinyurl.com/2s4fhcnj.
[16] Martin Gundersen, *Inside the Scam Network*, NRK (May 4, 2025), https://tinyurl.com/5n6cp2jd.
[17] Telegram is a free messaging service with over one billion monthly active users. Telegram channels are designed for one-way information sharing, where channel administrators can post in the channel to share information with channel members.

legitimate website and Magic Cat's AI tools collect the website's data and generate a fraudulent version. Those spoofed websites include logos and features of the real websites, including, for example, Google Play and YouTube logos, and links to those sites and features.

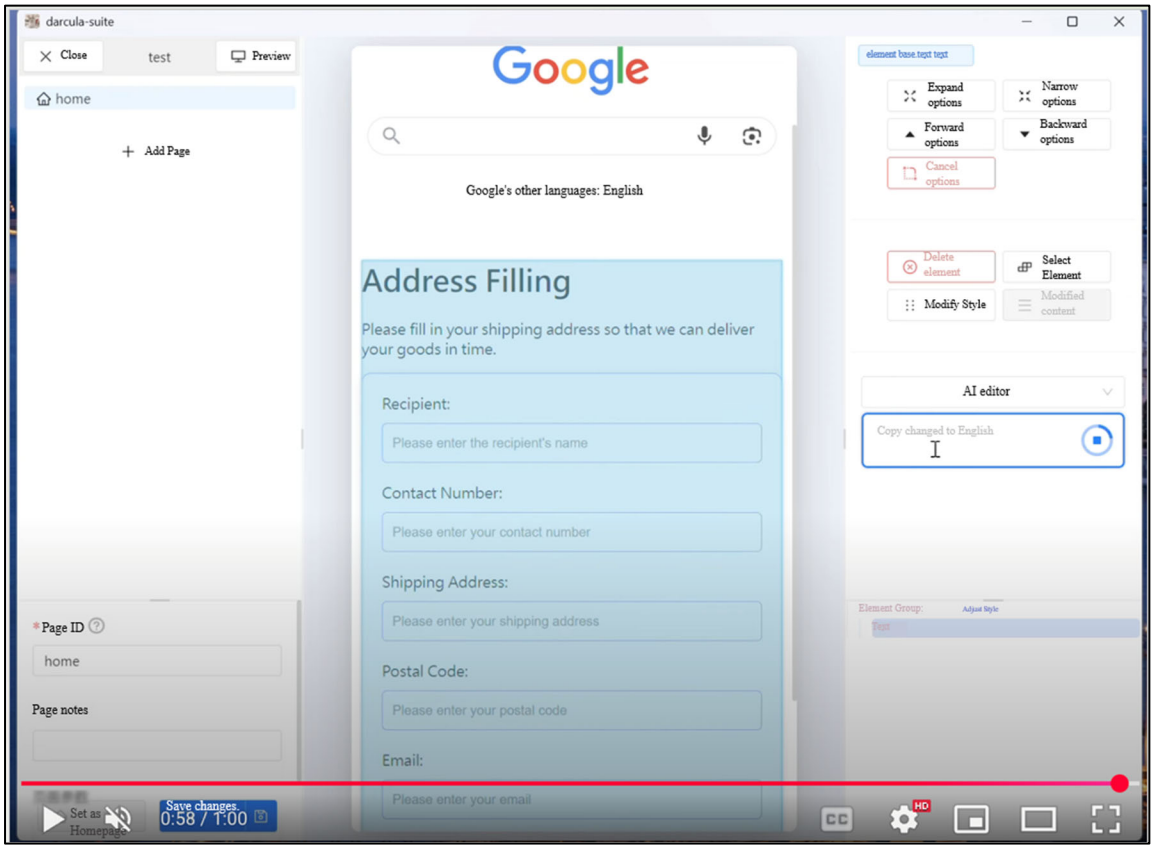
36. Magic Cat's built-in AI tool dramatically increases the threat posed by the Darcula Enterprise. Now, threat actors are not confined to the software's templates in determining which websites to duplicate in their phishing campaigns—they can mimic any website they believe will most effectively dupe their victims into providing personal and financial information.

37. In fact, Magic Cat includes a tutorial that demonstrates how to use the software. Those tutorial images show the software being used to spoof Google's homepage, Google.com, as shown below.



38. The Enterprise released another tutorial in April 2025 that again used a spoofed version of Google's homepage, Google.com, to demonstrate Magic Cat's new AI functionality.

To create a website that mimics Google's homepage, the Enterprise member copies data from Google's homepage into Magic Cat and then uses an AI tool to create a form purporting to collect address information. The form includes a request to "[p]lease fill in your shipping address so that we can deliver your goods in time." The Enterprise member can create the fillable form in Chinese and then use the Magic Cat "AI editor" box to translate the form into English, or another language of its choosing.



39. After generating a spoofed website, the Enterprise member sends the website's URL to targets through text messages, often called "bait" messages. Magic Cat's "bait" messages are deployed in text messages sent via Apple iMessage, RCS (the platform used by Google Messages), and SMS.

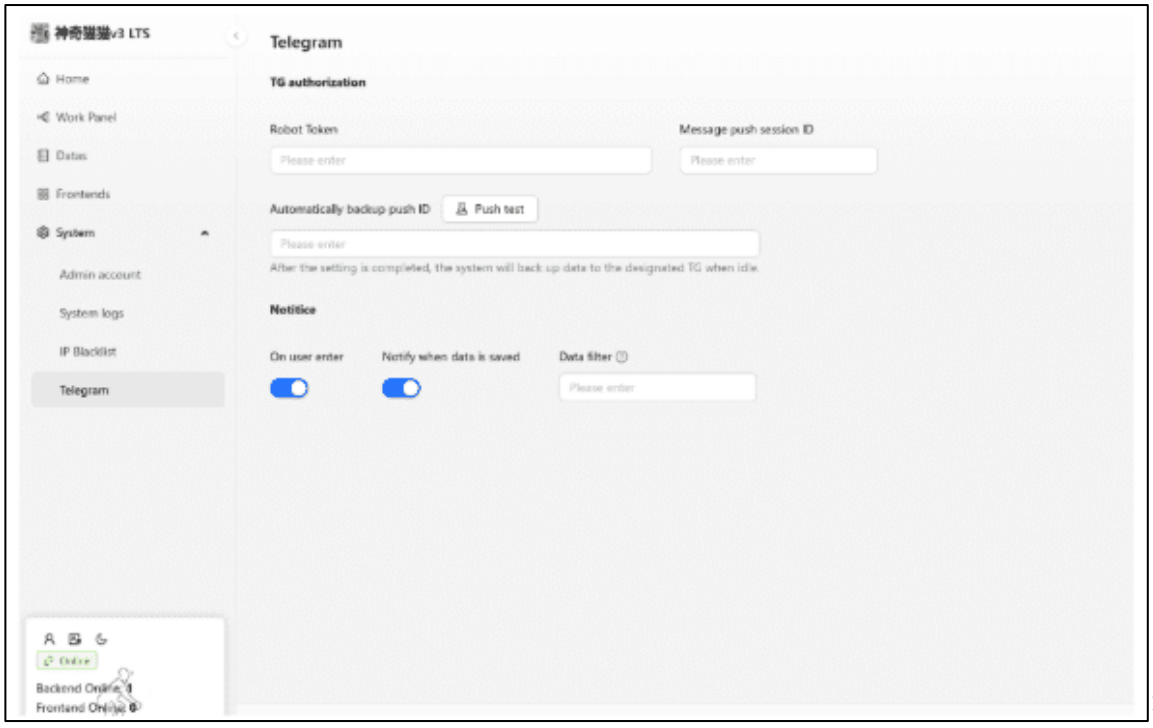
40. Using iMessage and RCS messages lends a veil of legitimacy to Magic Cat smishing attacks (where, for example, iMessage users may be more suspicious of "green" SMS

messages than "blue" iMessages), while simultaneously evading certain filters leveraged by SMS operators to block smishing messages.

41. Once the Enterprise member has used Magic Cat to generate and deploy "bait" in the form of phishing messages directing victims to fraudulent links, Magic Cat also provides the perpetrator real-time access to data entered by victims into the phishing websites by tracking the victim's keystrokes and relaying that information to the Enterprise member as the victim types.[18]

42. Magic Cat notifies the threat actor with a voice alert when a victim has accessed their fraudulent website and streams personal data to the threat actor as it is entered into the site.

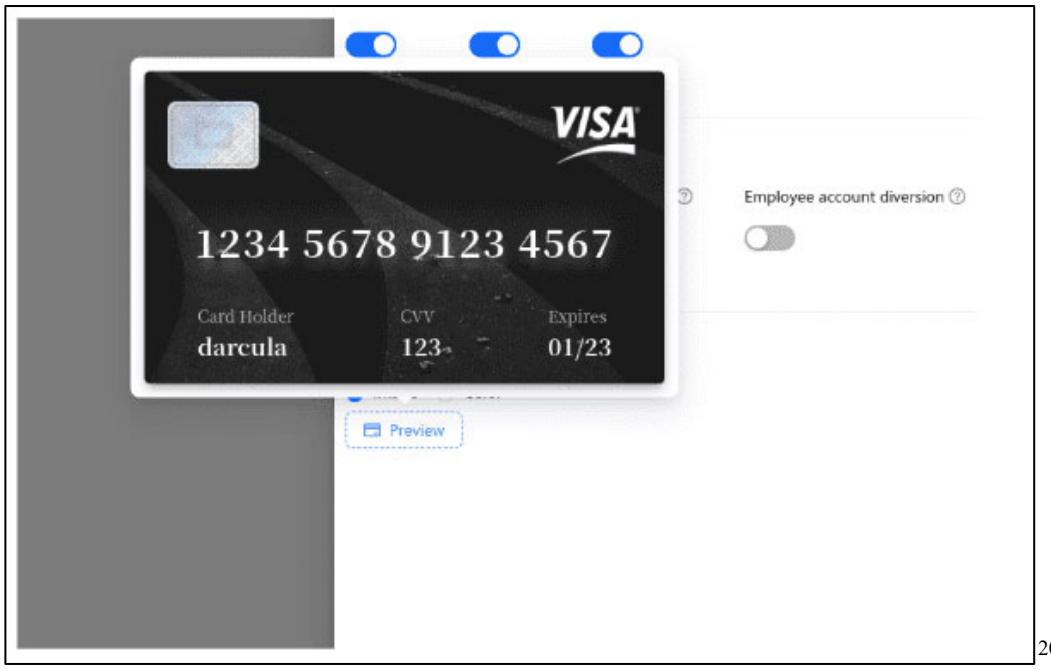
43. Magic Cat also offers integration with Telegram, allowing threat actors to receive notifications through that platform as well:



[19]

[18] Erlend Leiknes & Harrison Sand, *Exposing Darcula: a rare look behind the scenes of a global Phishing-as-a-Service operation*, Mnemonic (May 4, 2025), https://tinyurl.com/537tm5bs.
[19] Harry Freeborough, *The Bleeding Edge of Phishing: darcula-suite 3.0 Enables DIY Phishing of Any Brand*, NetCraft (Feb. 20, 2025), https://tinyurl.com/vmtu8h7h.

44. This suite of features allows cybercriminals with minimal technical expertise to steal victims' credit card numbers, financial account information, and personal data. But Magic Cat goes a step further in facilitating digital theft. Its program allows users to turn the stolen information into clones of victims' credit cards that can be added to digital wallets, as pictured below.



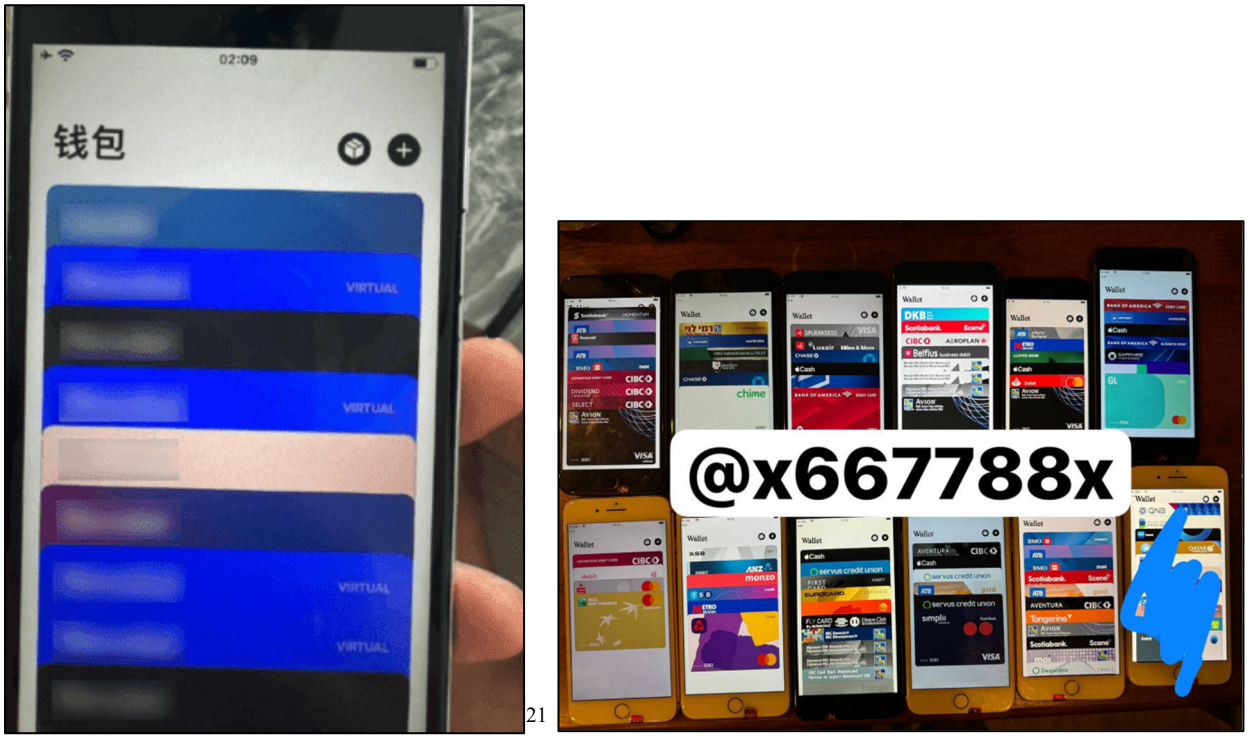
[20]

45. Members of the Darcula Enterprise commonly load these stolen cards onto burner phones they sell through illicit channels or use themselves for either online or in-person purchases using digital wallets like Google Pay's tap-to-pay technology.

46. Enterprise members have posted images to the Enterprise's Telegram community boasting about how they have stolen numerous credit cards, loaded those cards onto burner phones, and then offered those phones for sale. The photo on the left below is a picture that a member of

[20] *Id.*

the Enterprise posted that depicts a burner phone loaded with twenty stolen credit cards. The photo on the right depicts a dozen phones with stolen cards loaded onto digital wallets.



[21]

The Darcula Enterprise

47. The Darcula Enterprise includes several connected threat actor groups that design and implement complex criminal schemes targeting the general public. Although different members of the Enterprise play different roles, they all collaborate to execute phishing schemes that rely on the Magic Cat phishing software. None of the Enterprise's schemes can generate revenue without the cooperation of these groups. All the threat actor groups are connected to one another through historical and current business ties, including through their use of Magic Cat and the online community supporting its use, as described below. Although certain Enterprise members

[21] *Id.*

may serve multiple roles, the Enterprise is generally composed of members who participate in the following groups:

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

49. It includes the individuals or entities that develop and maintain Magic Cat by designing the software, architecture, and user interface, writing code to carry out its functions, and troubleshooting the software to ensure it works properly. The Developer Group is also responsible for providing ongoing maintenance, pushing out regular software updates, and integrating new features into the software.

50. The Developer Group includes, but is not limited to, individuals who operate under the Darcula alias, including Defendant Doe 1 a/k/a Yucheng Chang. When researchers contacted an email address associated with Chang, an individual acting under the alias "Lao Liu" confirmed that Chang "is employed by our company," that Chang was "one of the founders of Magic Cat," that "there are many people behind the program," and that Chang is "just one of the technologists who developed the program."[22] The individual also stated that while Chang "sells the most," "the income belongs to the company."[23]

51. In addition to performing routine maintenance on Magic Cat and providing troubleshooting and support tools to better enable threat actors to perpetrate phishing schemes, the Developer Group has launched two major upgrades to Magic Cat, dubbed "V2" and "V3."

[22] OSINT Industries Team, *Darcula and the Magic Cat: How OSINT Unmasked A Phishing Tycoon*, OSINT (Aug. 12, 2025), https://tinyurl.com/ypzjyuyu; Martin Gundersen, *The Hunt for Darcula*, NRK (May 8, 2025), https://tinyurl.com/42bj5esj.
[23] Martin Gundersen, *The Hunt for Darcula*, NRK (May 8, 2025), https://tinyurl.com/42bj5esj.

52. In V2, the Developer Group included hundreds of preloaded phishing templates for fraudulent websites mimicking U.S. government websites as well as the websites of major U.S. corporations.

53. In V3, the Developer Group added website customization and generative AI tools allowing Enterprise members to generate custom phishing templates, and redesigned the administrative dashboard to make it even more user-friendly.

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

55. Part of the appeal of the Magic Cat software is the ease with which someone with little technical expertise can purchase the software and immediately deploy a wide array of phishing attacks. That user-friendly appeal is enhanced by the tutorials, easily accessible instructions, technical support, and online community hosted on Telegram by the Administrative Group.

56. Between 2023 and early 2025, the Administrative Group created and managed a Telegram-based online community that was used to recruit new members of the Enterprise and to assist Enterprise members in using Magic Cat to carry out phishing attacks.

57. Some members of the Administrative Group also operate under the Darcula alias.

58. In one Darcula Telegram channel (@darcula_channel), members of the Administrative Group posted announcements regarding software updates as changes and improvements to the software were made available.

59. For example, on May 10, 2024, a member of the Administrative Group posted a video tutorial walking through the Magic Cat software features along with the post, "[t]here's a

little bit to look forward to, many parts have recently been standardized and rectified, laying the groundwork for the direction of future development."

60. The Administrative Group also used the @darcula_channel Telegram channel to promote and distribute resources for its phishing operations. For example, on July 2, 2023, a member of the Administrative Group posted, "Selling worldwide online data. Contact @pk520520 if needed."

61. On another Darcula-linked Telegram channel (@n9999n), members of the Enterprise record transactions they made. Additional channels have been used to promote Magic Cat by disseminating demonstrations of the software, to connect Enterprise members to allow them to collaborate on phishing schemes, and to enable Enterprise members to boast to other members about the success of their schemes.

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

63. These individuals or entities supply lists of potential victims' contact information to other members of the Darcula Enterprise, ensuring the wide reach of its many phishing schemes. Members of this group identify and compile contact information for potential victims and distribute the information for use in phishing attacks. One member of the Data Broker Group is user @pk520520, who shares international telephone numbers and contact information to Magic Cat scammers to enable their mass phishing schemes.

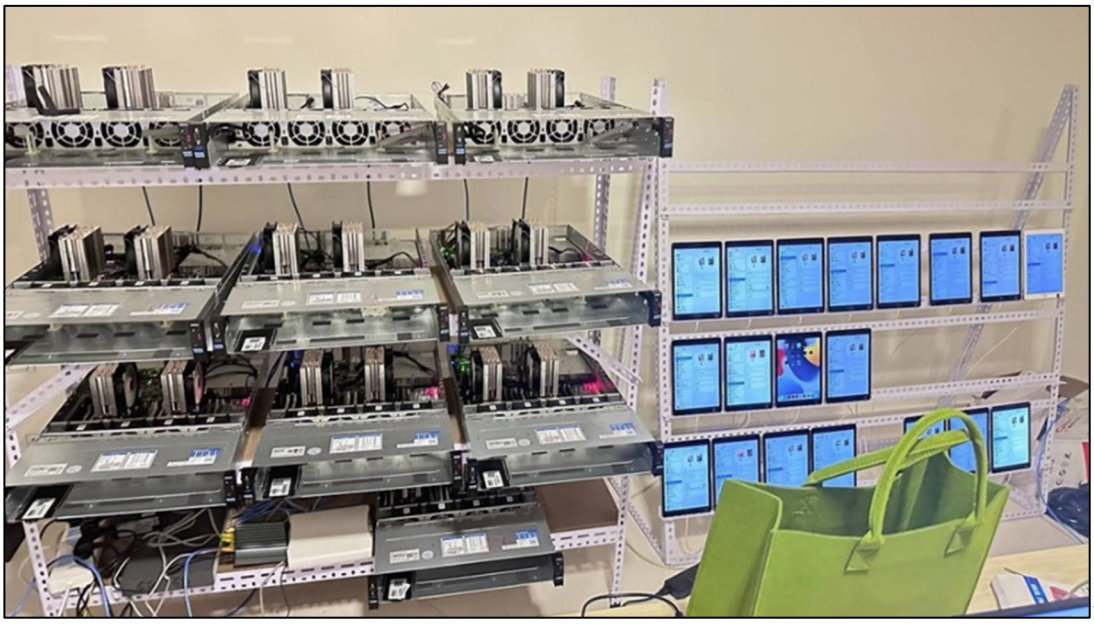
64. Another member of the Data Broker Group is user @xiaoyi990618, whose Telegram biography indicates that the user offers other members of the Enterprise products to facilitate phishing campaigns, including contact information for potential victims, the ability to

send bulk text messages to various devices, and point-of-sale machines allowing users to use stolen financial information to send money to themselves.

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

66. Large-scale smishing schemes require infrastructure to facilitate sending mass text messages. To send thousands of text messages simultaneously, the Enterprise needs banks of smartphones, SIM cards, modems, and services to support the data it demands. The Spammer Group provides these capabilities to other members of the Enterprise. For example, an individual, group of individuals, or entity acting under the username @x667788x helps send the messages necessary to contact victims of SMS scams—which often requires operating hundreds of cell phones at once.

67. Members of the Spammer Group shared the following pictures of their phishing "farms" on the Enterprise's Telegram channels, illustrating their operations:

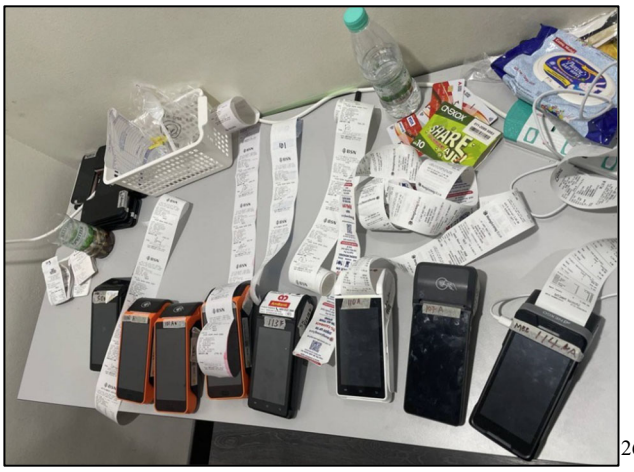
 [24]

[24] Erlend Leiknes & Harrison Sand, *Exposing Darcula: a rare look behind the scenes of a global Phishing-as-a-Service operation*, Mnemonic (May 4, 2025), https://tinyurl.com/537tm5bs.

 [25]

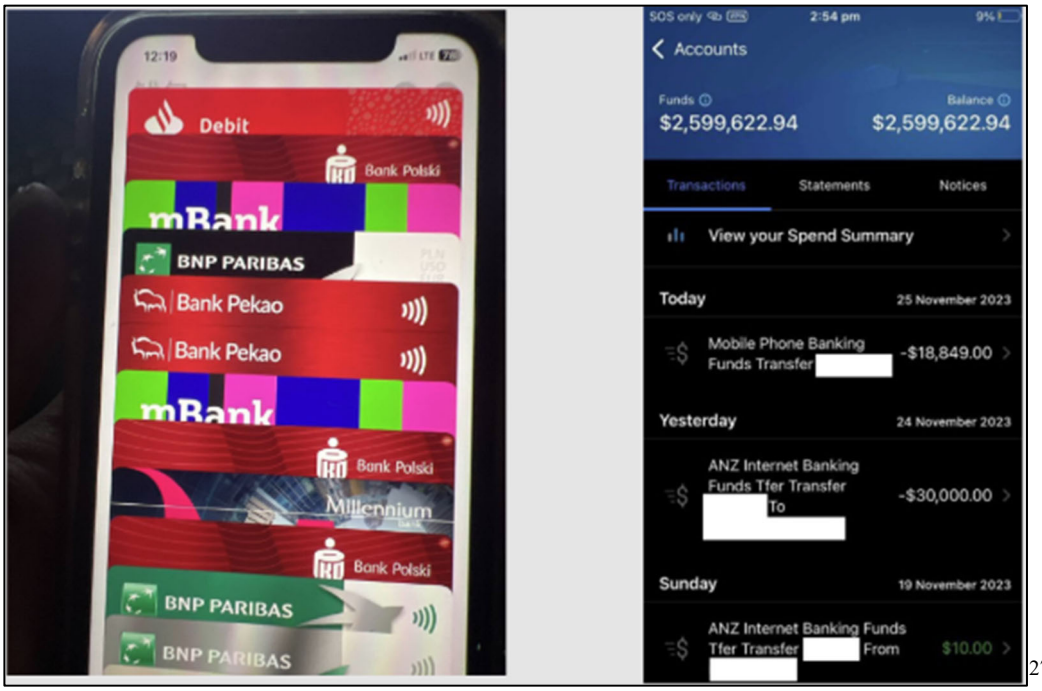
68. **The Theft Group:** Members of the Theft Group help to monetize stolen information.

69. These individuals or entities help steal money, social security information, and more once other members of the Enterprise acquire phished credentials from victims. For example, members of the Theft Group shared photos of payment terminals used to make purchases with stolen cards in the Administrative Group's Telegram channels, as shown below.

 [26]

[25] *Id.*
[26] *Id.*

70. With victims' credentials, the Theft Group can also access bank accounts, email accounts, brokerage accounts, and other sensitive accounts. These actors load stolen payment cards to digital wallets—like Google Wallet—and then resell phones containing the digital wallets that have stolen card information, which can be used to make purchases or launder money. Below are photos of digital wallets loaded with stolen credit cards and records of fraudulent transactions that Enterprise members shared in the Telegram channels.



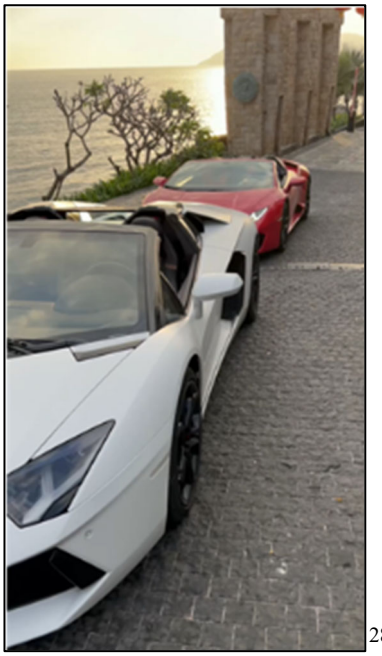
[27]

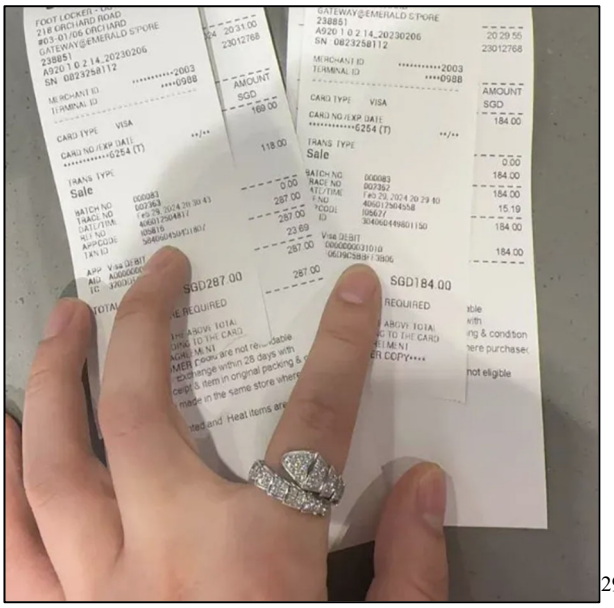
71. These groups coordinate with each other to recruit and train new members of the Enterprise, generate phishing strategies and tactics, select phishing targets, and coordinate phishing attacks. The Developer Group created the software and the Administrative Group markets it to recruit new members to the Enterprise. The Administrative Group also relays information about software updates to other members of the Enterprise and relays information from Enterprise members regarding software issues back to the Developer Group. Through the Administrative

[27] *Id.*

Group's Telegram channels, members of the Enterprise can plan phishing attacks and connect with the Data Broker Group and Spammer Group to utilize these groups' respective expertise and tools to execute attacks. Once the Enterprise has victim information in hand, the Theft Group monetizes, sells, or uses that information and helps to launder ill-gotten funds.

72. Working together, members of the Enterprise have amassed a significant amount of wealth and live a life of luxury funded by their victims. Members have posted about their success with the phishing schemes on social media, including on the Enterprise's Telegram channels:

 [28]

 [29]

73. Some members of the Darcula Enterprise have been described in investigative reporting published online. To avoid further detection, the Darcula Enterprise appears to have reduced its visible online presence for now, shuttering its Telegram channels and curtailing its efforts to expand. But Magic Cat's infrastructure remains intact and the Darcula Enterprise could resume its activities at any moment.

---

[28] *Id.*

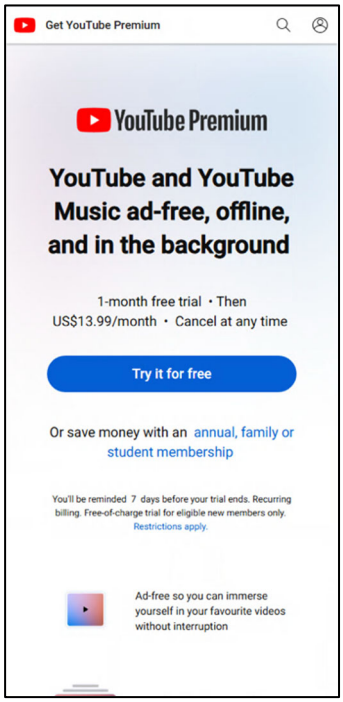
[29] Martin Gundersen, et al., *Inside the Scam Network*, NRK (May 4, 2025), https://tinyurl.com/5n6cp2jd.

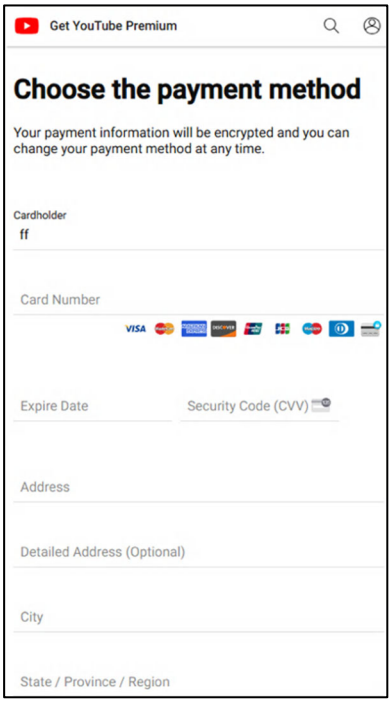
Fraudulent Schemes Executed by the Darcula Enterprise

74. Using Magic Cat, the Darcula Enterprise has been able to execute an astonishing number of phishing schemes. At its peak, researchers estimated that the Enterprise originated ***70 to 80% of all smishing messages***. Although Magic Cat includes templates for hundreds of fraudulent websites, several of the most well-known and commonly used smishing schemes include the YouTube Scheme, the Delivery Scheme, and the Toll Scheme.

75. **The YouTube Scheme:** The Darcula Enterprise has targeted Google by creating a template designed to spoof the YouTube Premium enrollment page.

76. In this scheme, an Enterprise member may use a template included with Magic Cat V2 to create a fraudulent version of the YouTube Premium webpage. The template includes both a fraudulent homepage and a page where "new users" are directed to provide their credit card information, purportedly to sign up for a one-month free trial to YouTube Premium. When a victim provides their financial information, however, they do not gain access to YouTube Premium; instead, an Enterprise member steals their financial information.

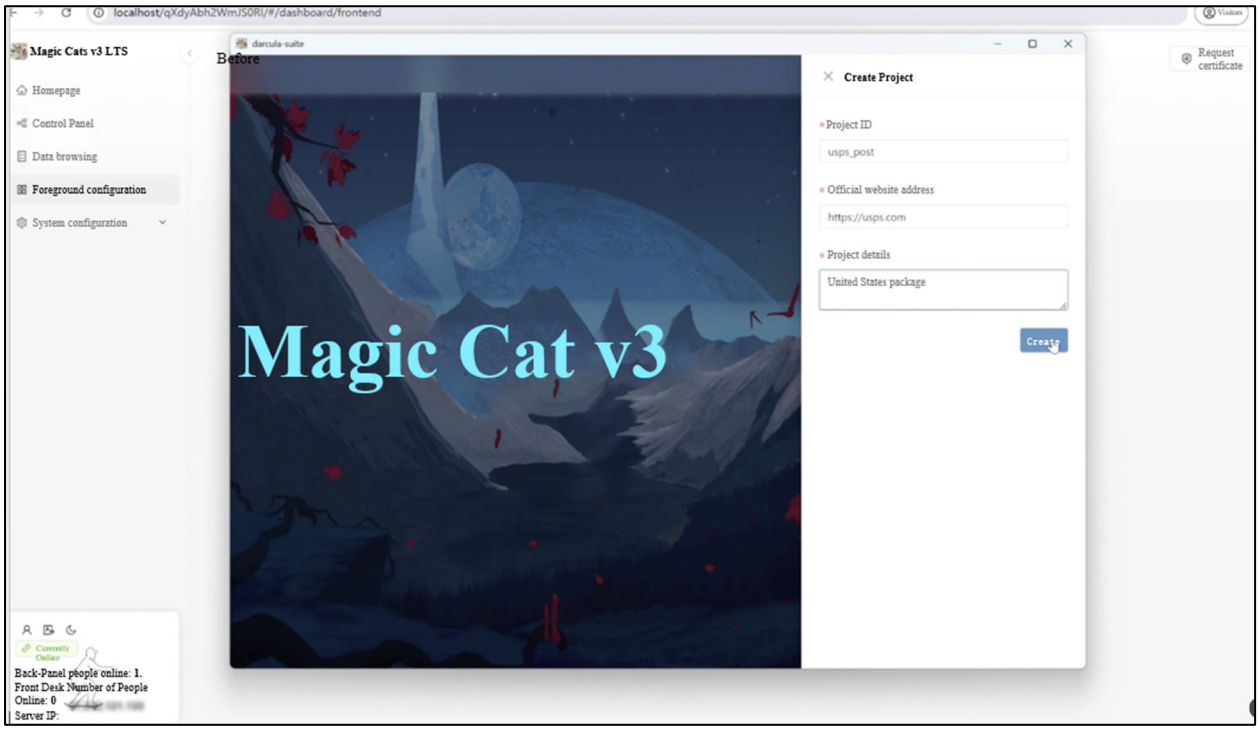




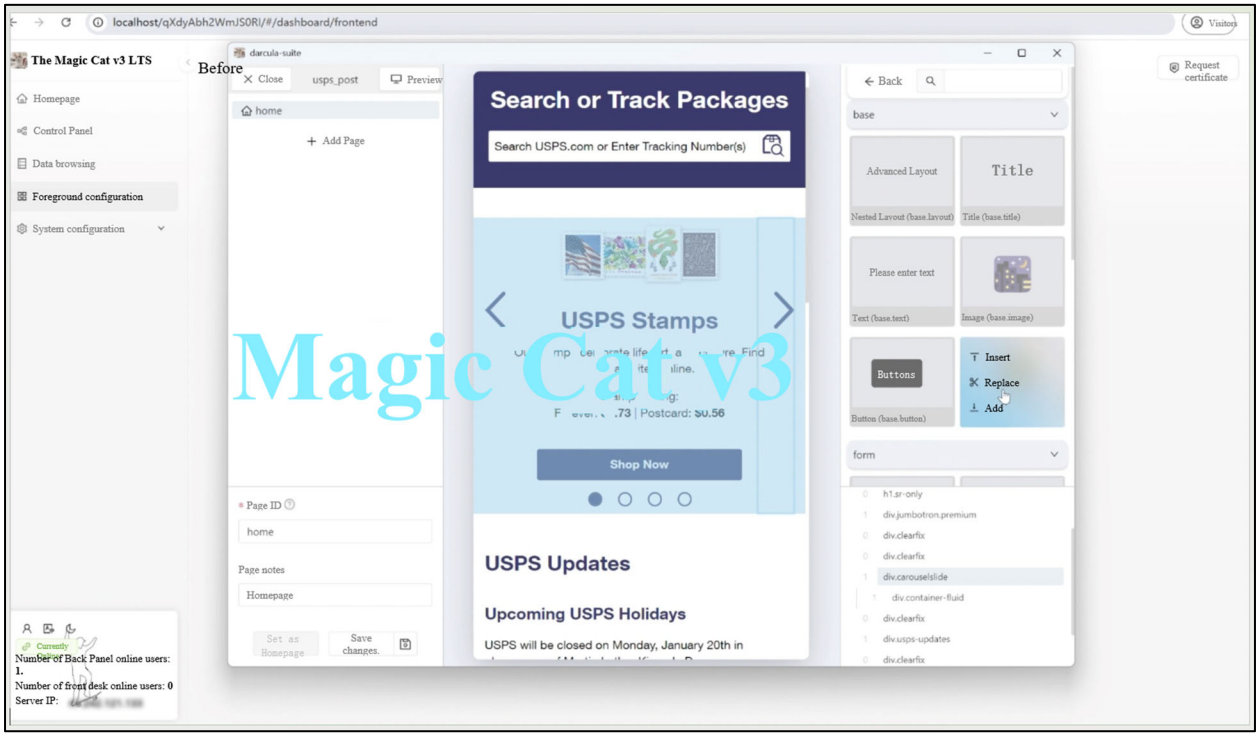
77. Members of the Enterprise collaborate to execute the attacks. For example, the Data Broker Group provides the Spammer Group with potential victims' phone numbers, and the Spammer Group in turn sends SMS or RCS messages in bulk to the phone numbers with links to the fraudulent webpage purporting to advertise a free trial to YouTube Premium. And once Enterprise members acquire victims' financial information, the Theft Group then provides opportunities to monetize the stolen personal and financial information, including by selling that information to other cybercriminals.

78. **Delivery Scheme:** The Darcula Enterprise's spoof of the USPS and other parcel delivery services is among the most common smishing attacks in operation.

79. To execute a delivery scheme using Magic Cat V3, members of the Enterprise first log in to a Magic Cat account and provide the URL that they would like to spoof, for example, https://usps.com:



80. Magic Cat sources images, text, and the website's design from the real USPS website, and creates a spoofed website that members of the Enterprise can edit and customize. An example is pictured below:



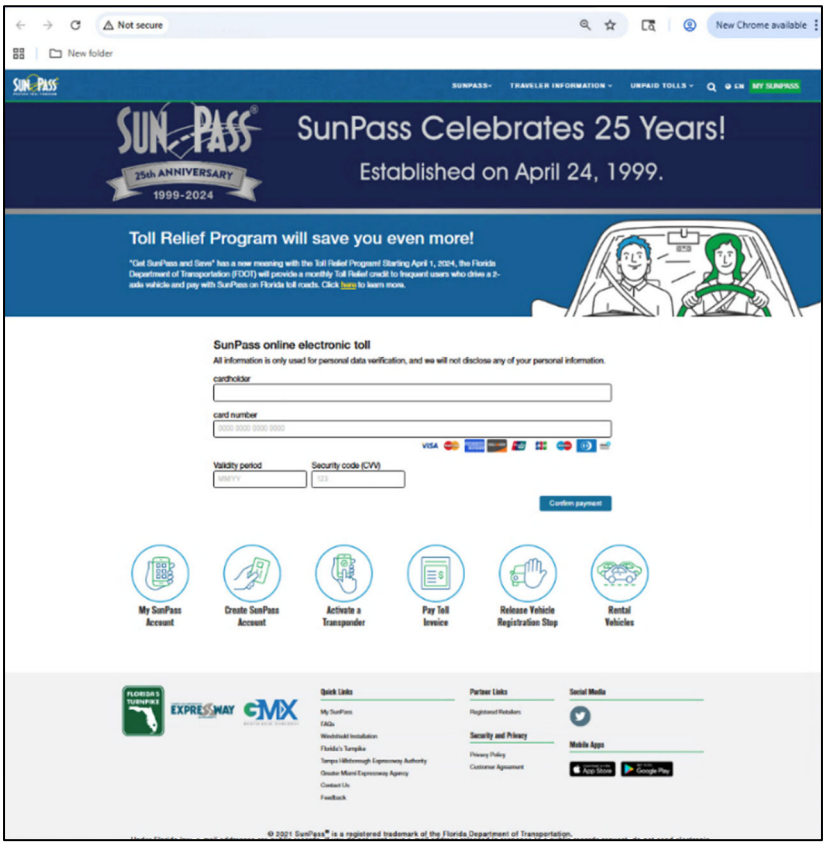
81. Once the spoofed website is customized, Enterprise members carrying out the attack can coordinate using the Enterprise's Telegram channels. For example, if Enterprise members are unable to transmit texts in bulk, they can retain members of the Spammer Group, who will send mass text messages for a fee.

82. The Darcula Enterprise then sends a carefully crafted text message to the targets, purporting to be USPS. Those texts are designed to convey a sense of urgency: in one example, they may purport to alert the target to a missed package delivery and include a link where the target can reschedule the delivery. If a target clicks the link, they are directed to a fake USPS website that requires payment of a small redelivery fee.

83. As the targets enter their personal financial details, the Magic Cat interface alerts the Enterprise through text messages or Telegram messages and simultaneously logs the target's keystrokes. The target need not actually submit the payment for the Enterprise to obtain the target's payment information. The Enterprise can then access that information on their Magic Cat account, where the software collects and organizes victims' stolen data, making it easier for the Enterprise to use that stolen data. Using the @darcula_channel on Telegram, the Enterprise posted a video tutorial that trains other Enterprise members to use Magic Cat to perpetrate the USPS scam.

84. **Toll Scheme:** Another common scam involves text messages purporting to pursue unpaid tolls.

85. Magic Cat includes hundreds of templates for fake websites, including many that replicate toll collection agencies. For example, Magic Cat offers a fake version of the Florida SunPass toll collection agency, pictured below.



86. In Magic Cat V3, Enterprise members can also simply input the URL for the SunPass website to create a fraudulent version of the website's most recent iteration. The fraudulent version of the website replaces the website page designed to collect payments with code that funnels credit card information directly to the Enterprise member who controls the page.

87. In this scheme, Enterprise members again coordinate to execute the attack. For example, once an Enterprise member creates a fraudulent website (using one of the fake toll collection templates available on Magic Cat V2 or V3, or creating a website for any toll agency using Magic Cat's AI functionality on V3), the Data Broker Group can provide the Spammer Group with potential victims' phone numbers, and the Spammer Group in turn sends SMS or RCS messages in bulk to phone numbers using phone banks, SIM banks, and other tools they possess.

88. The targets then receive a text message purporting to be a notice of a past-due toll invoice or ticket with a link to the fraudulent website. Like the delivery scam, the toll scam requests that targets input personal financial information, such as their credit card number, to pay the purported past-due toll.

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

Harm to Google, its Users, and the Public

90. The Darcula Enterprise causes significant harm to its victims by stealing their information and money. In the words of one Darcula smishing scam victim, "it's really all of us that pays for it[.] … I get irritated and angry. They have no honor or pride in life when they are stealing money that others have worked hard for. It is a disgrace to humanity."[30]

[30] Martin Gundersen, *The Hunt for Darcula*, NRK (May 8, 2025), https://tinyurl.com/42bj5esj.

91. The scope and impact of the Darcula Enterprise using the Magic Cat software is enormous. A recent cybersecurity investigation into the Darcula Enterprise revealed that, at its height, it included over 600 cybercriminals, each working to execute its fraudulent smishing schemes by sending tens of thousands of text messages to intended victims every day.[31] Since March 2024, the Darcula Enterprise has disseminated approximately 90,000 phishing websites.[32] In a period of just seven months, the Enterprise stole nearly 900,000 credit cards globally, with nearly 40,000 credit cards stolen from victims in the United States alone during that period.[33]

92. For almost three years, between 2023 and May 2025, the Darcula Enterprise operated openly through largely public online channels, apparently confident that its criminal enterprise was not vulnerable to disruption. But in May 2025, a team of journalists and cybersecurity experts published an in-depth report about the Darcula Enterprise, which caused the Enterprise to shutter many of its public communication channels and significantly reduce its public operations.

93. But Google's investigation has shown that the Enterprise is still active and working from the shadows, albeit on a smaller scale, creating and disseminating new phishing domains daily through Magic Cat.

94. In just a 25-day period between September 11 and October 5, 2025, for example, over 4,750 Google Messages users, including users in the United States, reported to Google

[31] Martin Gundersen, *Inside the Scam Network*, NRK (May 4, 2025), https://tinyurl.com/5n6cp2jd.
[32] *See* Harry Everett, *AI-Enabled Darcula-Suite Makes Phishing Kits More Accessible, Easier to Deploy*, Netcraft.com (Apr. 24, 2025), https://tinyurl.com/ms5a9m69.
[33] Davey Winder, *884,000 Credit Cards Stolen With 13 Million Clicks By A Magic Cat*, Forbes (May 6, 2025), https://tinyurl.com/3rudpxd6; Alexander Nabert et al., *The Chinese Scammers Behind the Fake DHL Messages*, BR24 (May 4, 2025), https://tinyurl.com/ymaj9zcs.

fraudulent phishing messages they received attempting to lure them into clicking on domains with spoofed websites created through Magic Cat.

95. For example, some messages read:

a. "Delivery is suspended because your delivery note does not include a house number. Please update as soon as possible";

b. "Your order details are incomplete or incorrect. Please review and update the information to avoid shipping delays"; and

c. "We've detected multiple attempts to log into your account. If this was not you, please block it."

96. In each instance, these messages are followed by links to phishing websites created by the Enterprise with Magic Cat.

97. Google's investigation into these thousands of fraudulent phishing messages to Google users identified hundreds of different phishing domains with spoofed websites that the Darcula Enterprise created and disseminated through Magic Cat.

98. Magic Cat's AI capabilities allow the software to be scaled to unprecedented levels. Any website can be replicated nearly perfectly, down to the brand logos of other products like Google Play or YouTube.

99. The Darcula Enterprise also harms Google by damaging customer trust and goodwill and forcing Google to devote significant time and resources to remediation efforts.

100. Specifically, the Darcula Enterprise targets Google Messages users by transmitting phishing messages through the RCS messaging protocol that Google has adopted in Google Messages.

101. The Enterprise has also prominently featured Google's branding and logos, specifically:

a. in Magic Cat tutorial videos used to instruct Enterprise members how to generate spoofed websites for use in their phishing schemes;

b. in a template spoofing YouTube Premium, specifically targeting Google's customers and impersonating Google itself through attacks using this template; and

c. in spoofed website templates featuring Google's branding or logos on the sign-in screens.

102. The Enterprise's template spoofing the Florida SunPass's website features the Google Play logo, telling targets that they can download the spoofed brand's app in the Google Play store. Multiple other Magic Cat-spoofed websites include the Google Play and YouTube logos (along with logos of prominent social media sites), mimicking a common feature of real websites to again create a veneer of legitimacy.

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

104. The exploitation of Google's product, branding, and logos harms Google's public image and may encourage customers to move away from using Google's products and services.

105. The use of these logos violates Google's Rules 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."[34] 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.[35]

106. The Enterprise also uses Gmail accounts to distribute phishing messages to potential victims using Apple devices through iMessages linked to these Gmail accounts. And the Darcula Enterprise frequently distributes these phishing messages to potential victims using Android devices through Google Messages (through RCS).

107. This use of Google products violates 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."[36] 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.

108. Google has invested significant resources to combat Magic Cat, the Enterprise, and other cybersecurity threats. Google has spent thousands of dollars and over 150 hours investigating and remediating the Enterprise's activities, including engaging teams around the world. And Google will have to continue these efforts as long as the Darcula Enterprise continues to develop, distribute, and deploy Magic Cat.

[34] Google, *Rules for Proper Usage*, Brand Res. Ctr., https://tinyurl.com/24dvmced (last visited Nov. 6, 2025).
[35] Google, *Google Play Legal Requirements*, Partner Mktg. Hub, https://tinyurl.com/2yz2mscd (last visited Nov. 6, 2025).
[36] Google, Terms of Service, https://tinyurl.com/ynm67nz3 (last visited Dec. 14, 2025).

CLAIMS FOR RELIEF

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

109. Google incorporates by reference the foregoing paragraphs (¶¶ 1–108) of the Complaint as if set forth in full.

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

111. 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).

112. 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).

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

The RICO Enterprise

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

115. As described *supra* at paragraphs 47 through 73, Defendants have organized themselves into a network of cybercriminals operating in the United States and overseas, targeting victims in the United States. Over time, they have adapted their operations and schemes, enlisted new threat actors in their operation, and expanded the scope and nature of their activities.

116. Utilizing Magic Cat to execute a wide variety of phishing schemes, Defendants act with the common purpose of enriching themselves and fraudulently obtaining sensitive personal and financial information. Specifically, Defendants have collaborated to establish, grow, manage, and deploy Magic Cat. To enrich themselves, members of the Enterprise all take part in directing the aspects of its phishing schemes: some develop and improve the Magic Cat software; others manage the Telegram channels where Magic Cat is marketed and sold and the Enterprise discusses their schemes; others supply lists of potential victims' contact information; still others share strategies for sending bulk text messages and identifying victims; and others help steal money, social security information, and more once other members of the Enterprise acquire phished credentials.

117. Defendants constitute an association-in-fact enterprise within the meaning of 18 U.S.C. §§ 1961(4) and 1962(c). The existence of this association-in-fact is evidenced by Defendants' membership and communication in the Enterprise's Telegram channels, common use of Magic Cat, coordination in executing phishing attacks, and the commercialization of the attacks, which indicates that Defendants function like a black-market business enterprise. *Supra* ¶¶ 47–89.

118. At all relevant times, the Darcula 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

119. At all relevant times, Defendants have conducted or participated in, directly or indirectly, the conduct, management, and/or operation of the Darcula Enterprise 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.

120. Defendants have directly or indirectly engaged in an unlawful pattern of racketeering activity involving thousands of RICO predicate offenses, including wire fraud in violation of 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.

121. 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' smishing schemes and by having to devote substantial financial resources to combat Defendants' criminal schemes. 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)

122. Defendants, with intent to defraud and obtain money or property by means of false or fraudulent pretenses, commit wire fraud in violation of 18 U.S.C. § 1343 by transmitting or causing to be transmitted, by means of wire communication in interstate or foreign commerce, writings, signs, and signals for the purpose of executing fraudulent schemes. Defendants have violated and continue to violate the wire fraud statute.

123. Defendants commit wire fraud in violation of 18 U.S.C. § 1343 each time that they send a fraudulent phishing message to an individual in the United States for the purposes of defrauding that individual into submitting sensitive personal and/or financial information through misrepresentation and deception in order to steal that individual's money or property. For example, the Darcula Enterprise misleads victims by using the names and websites of legitimate entities, such as USPS, to turn over that information, as described *supra* ¶¶ 78–80.

124. Between September and December 2025, over 5,000 Google Messages users reported to Google fraudulent messages they received from Defendants to perpetrate phishing schemes to steal money from these targets. For example:

a. On September 25, 2025, a U.S.-based Google Messages user reported receiving a phishing message from Defendants that stated, "We've detected multiple attempts to log into your account. If this was not you, please block it," followed by a link to a website domain created through Magic Cat to spoof the website of a U.S.-based financial institution.

b. On October 1, 2025, two different U.S.-based Google Messages users reported receiving a message from Defendants with text identical to the message quoted above, each followed by a link to a different website domain created through Magic Cat to spoof the website of the same U.S.-based financial institution.

c. On October 5, 2025, another U.S.-based Google Messages user reported receiving a message from Defendants with text identical to the message quoted above, again with a link to another website domain created through Magic Cat to spoof the website of the same U.S.-based financial institution.

d. On November 19, 2025, a U.S.-based Google Messages user reported receiving a phishing message from Defendants that stated, "Your updated 401(k) balance is ready to view. Please sign in for your most recent information," followed by a link to a website domain created through Magic Cat to spoof the website of a U.S.-based financial institution.

e. On November 27, 2025, another U.S.-based Google Messages user reported receiving a message from Defendants with text identical to the message quoted

above, again with a link to a website domain created through Magic Cat to spoof the website of the same U.S.-based financial institution.

125. Defendants sent each of these phishing messages through interstate or foreign wires with the intent to defraud the Google Messages user into entering his or her personal and financial information for the purpose of stealing money from his or her account.

126. Google has suffered direct injury to its business or property as a result of these wire fraud predicate offenses, including the substantial sums of money it has invested to investigate, remediate, and prevent these acts from being perpetrated on its customers and through its services.

Conspiracy to Violate RICO

127. Google incorporates the foregoing paragraphs (¶¶ 1–126) of the Complaint as if set forth in full.

128. 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).

129. Defendants knew that they were engaged in a conspiracy to commit multiple predicate offenses, and that the predicate offenses were part of a pattern of racketeering activity. Defendants' participation in the conspiracy and agreement to commit those offenses were 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).

130. Defendants agreed to direct or participate in, directly or indirectly, the conduct, management, or operation of the Darcula 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 Darcula Enterprise's affairs. The purpose of the conspiracy was to commit a pattern of racketeering activity

in the conduct of the affairs of the Darcula scheme, including the acts of racketeering set forth above, including the sale and use of Magic Cat to commit crimes, enriching the Enterprise.

131. 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.

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

133. 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)

134. Google incorporates the foregoing paragraphs (¶¶ 1–133) of the Complaint as if set forth in full.

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

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

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

138. Defendants used Google's Marks in connection with the advertising of services in commerce 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)

139. Defendants' and/or their agents' use of Google's Marks in commerce has caused and/or is likely to continue to cause confusion with Google's federally registered Marks, in violation of 15 U.S.C. § 1114(1). The use by Defendants and/or their agents of the Marks has caused and/or is likely to continue to cause confusion and mistake; has deceived and/or is likely to continue to deceive potential customers and the relevant purchasing public as to the source, origin, or sponsorship of Defendants' services; and has deceived and/or is likely to continue to deceive the public into believing that those services originate from, are associated with, or are otherwise authorized by Google, to the damage and detriment of Google's reputation, goodwill, and sales.

140. 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).

141. 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)

142. Defendants' and/ or their agents' use of the Google Marks in commerce has caused and/or is likely to cause confusion in violation of 15 U.S.C. § 1125(a)(1)(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.

143. 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).

144. 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)

145. 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).

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

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

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

149. 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.

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

151. 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).

152. 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.

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

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

154. Google incorporates the foregoing paragraphs (¶¶ 1–153) of the Complaint as if set forth in full.

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

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

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

158. Defendants' conduct involved interstate and/or foreign communications.

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

160. Specifically, Google has suffered loss as a result of Defendants' CFAA violations in the form of reasonable costs of responding to Defendants' scheme, including conducting damage assessments. *See* 18 U.S.C. § 1030(e)(11). Over the period from January 2025 to December 2025, those losses have exceeded $5,000.

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

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

PRAYER FOR RELIEF

WHEREFORE, Google prays for judgment as set forth below:

A. Judgment in favor of Google and against Defendants;

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

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

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

the activity complained of herein or from causing any of the injury complained of herein;

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

F. Judgment awarding Google actual and/or statutory damages from Defendants adequate to compensate Google for Defendants' activity complained of herein and for any injury complained of herein, including but not limited to interest and costs, in an amount to be proven at trial;

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

H. Judgment awarding attorneys' fees and costs; and

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

Dated: December 17, 2025

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

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

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

Counsel for Plaintiff Google LLC