

**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.:

**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, Google Search, YouTube, Google Cloud, Google Ads, Google Ad Manager, 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. [REDACTED]

[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 operating under the alias "Darcula" who use an end-to-end software called "Magic Cat" to perpetrate widespread phishing scams (the "Darcula Enterprise" or "Enterprise").

4. CCIG, working with other relevant Google teams, has assessed the activities of this phishing software and the impact it has 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 concluded that the Darcula Enterprise's use of Magic Cat has caused significant damage to Google, its customers, and victims of Darcula phishing attacks. Magic Cat is a powerful software that

utilizes artificial intelligence (“AI”) spoofing capabilities and 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 continues 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. We maintain our position at the forefront of multiple sectors through a sustained commitment to offering products that are both dependable and advanced, including ensuring our 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 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 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 created and operated by Google that runs on various operating systems, including on personal computers, smartphones, and tablets.
- c. **Google Ads:** Google Ads is an online advertising platform through which advertisers can publish advertisements on various platforms including, for example, Google Search and YouTube.
- d. **Google Ad Manager:** Google Ad Manager is a comprehensive ad management platform that allows publishers to sell ad space.
- e. **Gmail:** Gmail is an email service.
- f. **Google Cloud:** Google Cloud consists of a set of physical assets, such as computers and hard disk drives, and virtual resources, such as virtual machines, that are contained in data centers around the globe.
- 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 the official app store for certified devices running on the Android operating system and its derivatives, 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.

- i. **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.
- j. **Rich Communication Services ("RCS"):** RCS chats let users send messages over mobile data and Wi-Fi, share files and high-resolution photos. Messages sent using RCS chats use the RCS protocol, an industry standard for carrier messaging, and Google's RCS infrastructure. RCS chats between Google Messages are end-to-end encrypted by default to keep users' conversations secure.
- k. **YouTube:** YouTube is an online video sharing platform.

7. Each of these products and services, among others, contributes to the value of Google's brand—one of the most prominent and valuable brands in the world. The word "Google" itself has become a verb. 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 resources and guidelines governing the use of Google trademarks to ensure those trademarks are used to promote and not diminish Google's reputation. These efforts ensure that Google remains one of the world's most trusted technology brands.

## **II. Google's Commitment to Cybersecurity**

8. 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 whose work depends on our services. We strive to keep our 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.

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

10. Google has allocated, and continues to allocate, substantial resources to restricting phishing communications and protecting users on the web and mobile devices. These 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 preventing suspicious account sign-ins.

11. Google also has dedicated resources to thwarting attacks that result from the operation of 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 search to see whether a website is currently 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 set up correctly.

12. Because the cyber threat landscape is constantly evolving, Google has also devoted 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 the world relies on; and introduced Protected Computing, which transforms how, when, and where data is processed to technically ensure users' privacy and safety.

13. CCIG is central to all these efforts and focuses on protecting users from cybercrime on Google's platforms, with a particular focus on efforts to combat online fraud, phishing, and malware.

14. CCIG's work has been essential to disrupting numerous major cybersecurity threats, including significant botnet threats such as Glupteba,<sup>1</sup> Cryptbot,<sup>2</sup> BadBox, and BadBox 2.0,<sup>3</sup> and phishing threats like Lighthouse<sup>4</sup> and Darcula.

---

<sup>1</sup> Royal Hansen & Halimah DeLaine Prado, *New action to combat cyber crime*, Blog.Google (Dec. 7, 2021), <https://tinyurl.com/bde3v5fy>.

<sup>2</sup> Mike Trinh & Pierre-Marc Bureau, *Continuing our work to hold cybercriminal ecosystems accountable*, Blog.Google (Apr. 26, 2023), <https://tinyurl.com/pktdmsrc>.

<sup>3</sup> Google, *We're taking legal action against the BadBox 2.0 botnet.*, Blog.Google (July 17, 2025), <https://tinyurl.com/yc7jw5fm>.

<sup>4</sup> Halimah DeLaine Prado, *A dual strategy: legal action and new legislation to fight scammers*, Blog.Google (Nov. 12, 2025), <https://tinyurl.com/ycxbub5n>.

### **III. Phishing-as-a-Service and Magic Cat**

15. With other Google investigators, I investigate cybercrime campaigns like phishing-as-a-service (“PhaaS”) that are perpetrated by threat actors targeting Google and its customers. In this role, I have investigated the Darcula Enterprise and its PhaaS campaign.

16. Phishing is a type of cyberattack in which cybercriminals send emails, text messages, or electronic messages that impersonate organizations—including Google, its brands, and its logos—or individuals in order to trick the recipient of the attack into turning over sensitive information like passwords, credit card numbers, or banking information.

17. PhaaS turns this criminal activity into a business model—cybercriminals sell software and support services to better facilitate phishing schemes. The software, also sometimes referred to as a “phishing kit,” provides the infrastructure necessary to create a fake website (or other platform), send bulk text messages and emails to victims, and collect and store stolen personal and/or financial information. A typical phishing kit may include ready-made text message templates, 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. The kits are essentially a guide to phishing, and they 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.

18. The Darcula Enterprise’s phishing software, referred to as “Magic Cat,” is composed of two complementary components. The first part, called the “darcula-suite” software, is the front-end software that is installed on the phishing kit user’s computer and allows the user to make and revise phishing websites. The second part is a server-based program, called Magic Cat. This part allows users to deploy phishing sites and collect stolen information from victims.



Typically, the entire software package is referred to as “Magic Cat,” so I will refer to the software as Magic Cat other than when I am specifically referring to the darcula-suite front-end software.

19. Phishing kits, like Magic Cat, make cybercrime easier for less technically skilled perpetrators to commit because they can rely on a product that does all the technical work for them. Additionally, these kits make cybercrime cheaper because cybercriminals do not need to expend significant financial resources to develop and scale their infrastructure. The PhaaS model is lucrative because it enables widespread and fast-paced phishing activities.

20. The Darcula Enterprise’s Magic Cat software allows its network of scammers to create and deploy fraudulent websites—which spoof the legitimate websites of YouTube and other well-known organizations and businesses—with ease. The Darcula Enterprise distributes links to these spoofed websites in phishing attacks initiated through iMessages, RCS messages, and SMS messages.

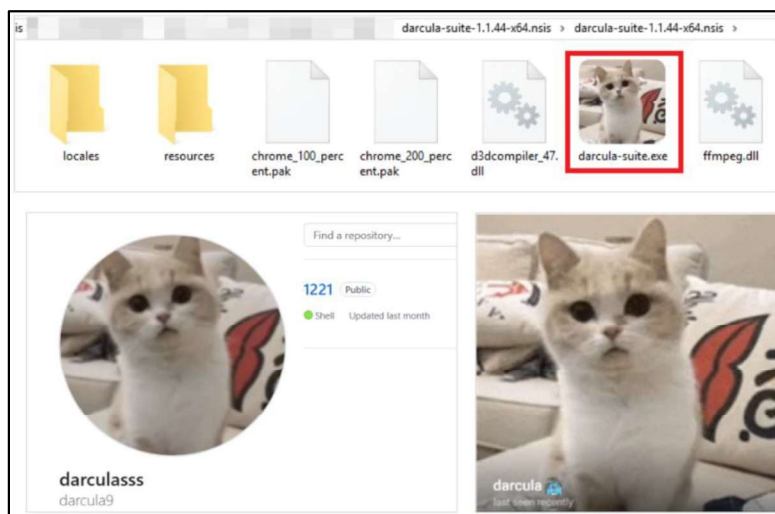
21. As victims type their personal and/or financial information into the spoofed website, Magic Cat collects the information and sends it directly to the Darcula Enterprise in real time.

22. Through the Darcula 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 Darcula Enterprise’s Phishing Scheme**

23. Through its investigation of the Darcula Enterprise, Google obtained a copy of the source code for the Magic Cat software from VirusTotal on May 6, 2025. VirusTotal is a free, Google-owned online service that analyzes suspicious files, URLs, IP addresses, and domains for malware and threats using dozens of antivirus engines and threat intel feeds. Users can upload or

input items to be scanned, and the service aggregates results from multiple sources to provide a comprehensive safety assessment. The source code file “darcula-suite-1.1.44-x64.nsis.7z” (file size 93.81 MB) is available on VirusTotal with the first seen date of “2025-05-06 21:41:45 UTC.” The source code file contains a desktop application called “darcula-suite” built with Electron framework (an open-source software framework that enables developers to build cross-platform desktop applications using web technologies like HTML, CSS, and JavaScript). The icon for the desktop application, shown below, is a cat picture that is identical to that used to identify other Darcula infrastructure, such as one of Darcula’s Telegram administrative profile pictures and one of Darcula’s GitHub repositories used to host the phishing templates.



24. VirusTotal logs the URLs outside of VirusTotal where the file is being used (known as an ITW URL or “In-the-Wild” URLs). Based on the ITW URLs for “darcula-suite,” my team concluded that the source code file was hosted at “[https://gitlab\[.\]com/magic-cat-v3/repo/-/raw/main/darcula-suite-1.1.44-x64.nsis.7z](https://gitlab[.]com/magic-cat-v3/repo/-/raw/main/darcula-suite-1.1.44-x64.nsis.7z).”

25. My team also acquired phishing templates from the Github repository located at the following URL: [https://github\[.\]com/feixiang8956/Darcula-phishing-CVV-Logs](https://github[.]com/feixiang8956/Darcula-phishing-CVV-Logs). We

downloaded the “.cat-page” file containing the phishing templates. The “.cat-page” file can be imported into the “darcula-suite” desktop application to create custom phishing pages.

26. Google has also worked to identify fraudulent website domains that were created using the Magic Cat software. By analyzing the source code and phishing templates, my team identified two unique fingerprints for Magic Cat. One of the files in the Magic Cat source code titled “/app/chunk/” contains two scripts (“DgZYu39z.js” and “IB9GikLJ.js”). Together these scripts handle the encryption and decryption of messages sent and received from Magic Cat’s command-and-control server via API endpoints and WebSockets. Both scripts have a unique name that never changes so they can be used to identify sites that use Magic Cat. In addition, both scripts contain references to “darcula.”

27. My team provided the source code and phishing templates discussed above to our research partner NAXO for further investigation.

28. Based on cybersecurity researchers’ public reporting about their investigations into the Darcula Enterprise, Google identified Gmail accounts used by members of the Darcula Enterprise. Based on billing instruments associated with these accounts, Google determined that an individual whose name is likely Yucheng Chang used some of these Gmail accounts. Google’s analysis of the billing records associated with these Gmail accounts indicate that this individual resides in China. These findings from Google’s investigation are consistent with the public reporting on the Darcula Enterprise, which identified an individual named “Yucheng C.” as one of the leaders of the Enterprise.<sup>5</sup> In my experience, however, individuals involved in phishing schemes often use fake or stolen information; for that reason, Google does not know the Defendants’ true identities.

---

<sup>5</sup> Martin Gundersen, *The Hunt for Darcula*, NRK (May 8, 2025), <https://tinyurl.com/42bj5esj>.

## **V. The Darcula Enterprise's Use of Google Trademarks and Products**

29. The Darcula Enterprise uses free Google tools to carry out phishing schemes. For example, Darcula Enterprise members have created Gmail accounts to distribute the 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).

30. The Darcula Enterprise also uses victims' stolen credit card information by adding those stolen credit cards to Google Wallets on burner Android devices.

31. The Darcula Enterprise's conduct violates Google's Terms of Service, which prohibit "accessing or using our services in fraudulent or deceptive ways, such as ... phishing" or "creating fake accounts."<sup>6</sup> Although the identified accounts have been closed, I have directed my team to shut down any Enterprise-run Gmail accounts alongside Google's other disruption efforts.

32. Darcula also distributes hundreds of templates to create phishing websites that spoof the legitimate websites of YouTube as well as other reputable organizations and businesses, like the United States Postal Service, to encourage victims to enter their sensitive personal and financial information. Many of these spoofed phishing websites mimicking the websites of other reputable organizations and businesses also feature Google's trademarks for products such as YouTube or Google Play on the sign-in screen.

33. In addition, the most recent version of Magic Cat created and distributed earlier this year by the Darcula Enterprise uses AI to create a spoofed version of any website in minutes without any technical expertise required.

---

<sup>6</sup> Google, *Terms of Service* (last visited Dec. 14, 2025), <https://tinyurl.com/4f59tyr9>.

34. In April 2025, the Enterprise made a tutorial video demonstrating Magic Cat’s new AI functionality. In that video, the Darcula Enterprise used Google’s homepage (Google.com) to showcase how Magic Cat could create, in a matter of minutes, a spoofed version of the web page that could facilitate a new phishing scheme.

35. A list of Google trademarks the Darcula Enterprise has used without Google’s permission in its cybercrime activities is attached as **Appendix B**.

36. The use of these logos violates Google’s Rules for Proper Usage of its trademarks and brand features, 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.”<sup>7</sup> 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.<sup>8</sup>

37. Due to Google’s reputation of providing secure internet products, victims may view the presence of a Google trademark as an indicator that the website is safe or legitimate. The Darcula Enterprise is using the Google branding—and the goodwill associated with it—to convince victims to turn over their sensitive financial data.

## **VI. The Darcula Schemes Are Causing Harm to Google, Its Users, and the Public**

38. The Darcula Enterprise’s criminal actions have impacted Google, its users, and millions of other persons and entities.

---

<sup>7</sup> Google, *Rules for Proper Usage*, Brand Resource Ctr. (last visited Dec. 14, 2025), <https://tinyurl.com/fppdbffw>.

<sup>8</sup> Google, *Google Play Legal Requirements*, Partner Mktg. Hub (last visited Dec. 14, 2025), <https://tinyurl.com/4vd29caf>.

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

40. Between September 10 and December 3, 2025, over 5,000 Google Messages users—from the United States and other countries throughout the world—reported to Google fraudulent phishing messages they received from the Darcula Enterprise containing links to phishing website domains created through Magic Cat. 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 identical text, 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 identical text, again with a link to a 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 identical text, again with a link to a website domain created through Magic Cat to spoof the website of the same U.S.-based financial institution.

41. More than 200 different known spoof website domains of the Darcula Enterprise were used across these more than 5,000 phishing messages to Google users. In response to the phishing messages, Google has taken action to block further Google Messages from being distributed by the phone numbers and/or accounts used to send these phishing messages.

42. Google has devoted (and continues to devote) substantial resources to detect, deter, and disrupt the Enterprise’s activities. Google has done so because the use of Magic Cat poses a threat to Google’s brand and reputation, and forces Google to devote resources to fraud-protection activities like flagging malicious websites and Google Messages sent through RCS.

43. Google has spent at least 150 hours investigating and remediating Defendants’ activities, including engaging teams across four different countries. And Google will have to continue these efforts as the Darcula Enterprise’s activities continue. The cost of investigating the Darcula Enterprise, assessing the damage it causes, and determining whether any remedial measures are needed, have far exceeded \$5,000 in less than a one-year period from January 2025 to present.

44. Despite Google's best efforts, the Darcula Enterprise's continued cybercrime poses an imminent and irreparable injury to Google's business and reputation.

45. Beyond Google, the continued proliferation of phishing, smishing, and PhaaS is a threat to the public as whole.

46. Due to its sophisticated nature, I believe that if the Darcula Enterprise were given advance notice that the website domains and IP addresses they use in their phishing operation would be disabled, the Darcula Enterprise would take measures to ensure the phishing operation's survival and frustrate any disruption efforts.


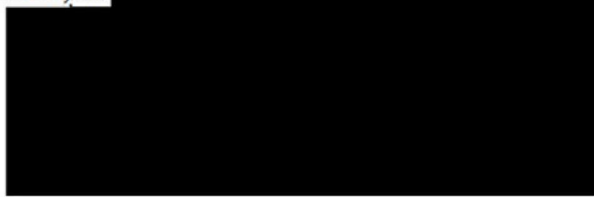
47. Based on my experience and the information currently known, I believe the most effective way to address the harm caused by the Darcula Enterprise is to:

- 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 Darcula Enterprise, not to warn or aid the Darcula Enterprise, and not to enable circumvention of the order; and
- c. Block any efforts by the Defendants to create any additional domains.

48. 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 Darcula Enterprise's harmful activities.




49. If the use of Magic Cat is not disrupted, it will continue to proliferate. The Darcula 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 December 16, 2025, in   


# Appendix B

**Appendix B**  
**Google Registrations Implicated by the Darcula Enterprise**

No.	Mark	Status / Dates
1	 RN: 4838524 SN: 86977379	Registered & Incontestable  First Use: August 19, 2013 Filed: June 20, 2014 Registered: October 20, 2015
2	 RN: 5581035 SN: 86316342	Registered & Incontestable  First Use: August 19, 2013 Filed: June 20, 2014 Registered: October 9, 2018
3	 RN: 5365541 SN: 86915697	Registered & Incontestable  First Use: September 1, 2015 Filed: February 22, 2016 Registered: December 26, 2017
4	GOOGLE  RN: 2806075 SN: 75978469	Renewed & Incontestable  First Use: September, 1997 Filed: September 16, 1999 Registered: January 20, 2004 Last Renewal: January 20, 2024

No.	Mark	Status / Dates
5	GOOGLE RN: 6373292 SN: 87786172	Registered First Use: September, 1997 Filed: February 6, 2018 Registered: June 1, 2021
6	 RN: 4058966 SN: 85222261	Renewed & Incontestable  Registered: November 22, 2011 Last Renewal: November 22, 2021
7	 RN: 5324610 SN: 86912587	Registered & Incontestable  First Use: September 1, 2015 Filed: February 18, 2016 Registered: October 31, 2017
8	 RN: 5324609 SN: 86912574	Registered & Incontestable  First Use: September 1, 2015 Filed: February 18, 2016 Registered: October 31, 2017
9	GOOGLE PLAY RN: 5570801 SN: 85560994	Registered & Incontestable  First Use: March 6, 2012 Filed: March 5, 2012 Registered: September 25, 2018
10	 RN: 5628029 SN: 85563165	Registered & Incontestable  First Use: April 14, 2016 Filed: March 7, 2012 Registered: December 11, 2018