UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

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

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

I, [redacted], declare as follows:

1. My name is [redacted]. I am over eighteen years of age and competent to testify to the matters set forth herein.

2. I am a member of NAXO Labs LLC ("NAXO"), a company that conducts blockchain and cyber investigations in connection with civil and criminal litigation. At NAXO, I manage and oversee crypto asset, dark web, and related investigations. Before joining NAXO, [redacted], I used my technical expertise in blockchain and the dark web to investigate a wide range of cyber- and crypto-related crime, including crimes against children, financial crimes, and network intrusions. I also led investigations identifying, locating, and apprehending criminals who used decentralized networks to obfuscate their identities. Among other matters, I led a multi-year investigation that resulted in the identification, apprehension, and conviction of two individuals who operated one of the most heavily trafficked criminal sites on the dark web. After apprehending the site's administrators, I

led the effort to use their accounts to identify and arrest a large network of offenders operating on the dark web.

3. Prior to my time at [redacted]. There, I was responsible for investigating financial crimes and cybercrimes and recovering electronic evidence from seized devices. I also served as a [redacted], where I used data analysis to investigate complex federal contract fraud.

4. I hold a [redacted].

5. Over the course of my career, I have testified as an expert in the areas of access device fraud, financial crimes, digital forensics, and cybercrime investigations in legal proceedings on several occasions, including testimony at trials, before grand juries, and in hearings at both the federal and state levels.

6. In support of the accompanying Complaint, I conducted an investigation of phishing software known as "Lighthouse." The software enables criminal actors to steal personal information and financial data from victims by creating fake websites that closely resemble legitimate websites. When victims enter their personal and/or financial data into the fraudulent websites, that data is funneled to the users of Lighthouse. The Lighthouse users then appropriate the stolen information for personal financial gain, either by exploiting victims' financial accounts themselves or by selling bulk collections of stolen data to other criminal networks. Lighthouse is pervasive and pernicious—it has been used to create thousands of phishing websites, leading to

the theft of financial information from tens of thousands of victims and losses of potentially millions of dollars.

7. The Lighthouse software was created by a person or persons going by the name of Wang Duo Yu (a.k.a. Lao Wang) using the Telegram username @wangduoyu0. Wang Duo Yu is part of a network of criminals, including those with Telegram usernames @fyy8588 (a.k.a. CoSmile), @Gblockduoyu (a.k.a. Kunlun), @xiaobai77699 (a.k.a. Nutbrownbear), and others who help sell and market the Lighthouse software and facilitate communication channels so that other members of the network can connect with each other to engage in phishing schemes. My investigation involved reviewing public information including online chat forums, communicating with Telegram user @wangduoyu0, collecting phishing websites created by Lighthouse, and analyzing Lighthouse itself.

8. I have been retained by Google LLC to conduct the investigation described herein. I am being compensated at a rate of $625 per hour. The opinions I am providing are my own and are not contingent on my compensation or the outcome of this matter.

I. Background Terminology

9. Phishing is a cybercrime in which attackers impersonate legitimate entities to trick people into clicking on a link or navigating to a website built to steal sensitive personal information. Phishing messages are typically delivered through email, text message, or targeted online advertising. Commonly impersonated entities include financial institutions, postal and shipping companies, government agencies, and cryptocurrency exchanges. Phishing attacks target personal data, usernames and passwords, and banking and credit card information.

10. Phishing-as-a-service is a term that describes a business model that sells software and support services to facilitate phishing, making it relatively easy for those without technical

expertise to create a phishing campaign. The phishing 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. For example, phishing software may contain ready-made website templates that closely resemble legitimate websites.

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

12. E-commerce phishing scams use websites that purport to sell products but instead serve the primary purpose of collecting credit card details and other information for fraudulent uses. These websites sometimes impersonate legitimate retail websites. Scammers often direct customers to these websites through advertisements on social media platforms or by sending email messages.

13. Telegram is a free messaging service with over one billion monthly active users.[1] Users typically create Telegram accounts with a phone number and can set a unique Telegram username.[2] Telegram allows users to directly message each other and join conversational groups with up to 200,000 members.[3] Typically, any member of a group can post in that group. Users can

[1] *See* Katherine Li, *Telegram Hits 1 Billion Active Users as CEO Pavel Durov Takes Swipe at Meta-Owned Rival WhatsApp*, Business Insider (Mar. 19, 2025), https://tinyurl.com/msn92bku.
[2] *See No-SIM Signup, Auto-Delete All Chats, Topics 2.0 and More*, Telegram.org Blog, https://tinyurl.com/3akd4xdm.
[3] *See Group Chats on Telegram*, Telegram.org Blog (Jan. 29, 2018) https://tinyurl.com/vppe886w.

also join Telegram channels, which are designed for one-way information sharing. Usually, only channel administrators ("admins") can post in a channel.[4] Any user can create new Telegram groups and channels.

14. Multi-factor authentication ("MFA") is an account security measure that requires enhanced verification to access an account in addition to a username and password. Most commonly, this is a one-time passcode sent to an account holder's email or phone.

15. 3-D Secure refers to a security technology implemented by many credit card issuers that aims to reduce online fraud. When a user attempts certain actions with the credit card, like making an online payment or adding a credit card to a mobile wallet, the card issuer can request additional authentication (MFA) from the user. Brand names of this type of technology include Visa Secure,[5] Mastercard Identity Check,[6] American Express SafeKey,[7] Discover ProtectBuy,[8] and Google Secure Payment Authentication.[9]

16. An Internet Protocol ("IP") address is a unique set of numbers and sometimes letters assigned to devices connected to the internet, allowing connected devices to communicate with each other.

17. Domains or domain names are human-readable addresses for a website that replace numerical or alphanumeric IP addresses, like www.google.com.

---

[4] *See Telegram Channels*, Telegram.org Blog (Jan. 29, 2018), https://tinyurl.com/8aajwsk9.
[5] *See Visa Secure with EMV 3-D Secure Authentication*, Visa Online Payment Fraud, Emerging Threats, Segment Analysis Market Forecasts (Nov. 2018), https://tinyurl.com/bde43zrb.
[6] *See Identity Authentication, Ensure Your Customers are Real*, Mastercard Cybersecurity and fraud prevention, Identity (2025), https://tinyurl.com/2wdzhxz9.
[7] *See American Express SafeKey & Online Safety*, American Express.com (last visited Nov. 6, 2025), https://tinyurl.com/257r5nfv/.
[8] *See 3DS ProtectBuy, Reduce the Growing Threat of Card-Not-Present Fraud*, DiscoverGlobalNetwork.com (last visited Nov. 6, 2025), https://tinyurl.com/3yywej6j.
[9] *See* Jose Ugia, *What's New in Google Pay*, Google for Developers (May 23, 2023), https://tinyurl.com/4hypr6s4.

18. Crypto assets are digital assets that exist only in electronic form and rely on cryptography to facilitate and validate transfers of value from one party to another. Bitcoin, first introduced in a 2008 whitepaper, is generally considered to be the first widely adopted crypto asset.[10] Users of crypto assets are represented by "addresses," virtual locations from which crypto assets are sent and received.

19. USDT is a crypto asset that is available on multiple blockchains. It is issued by Tether and is a "stablecoin," meaning that it aims to be priced at or near one U.S. dollar.[11]

II. Overview of the Lighthouse Phishing Software

20. People who use mobile phones or the internet are regularly targeted by scammers attempting to steal their account logins or financial information. Potential victims receive text messages directing them to click on a link; open emails pretending to be from real businesses or contacts; or accidentally navigate to websites that look almost identical to those of legitimate companies. If internet users are not careful, these text messages, emails, or even their own browsing can lead them to malicious websites. These websites "spoof" those of legitimate companies and are built to look and function the same as the trusted websites people visit daily. When scam victims are fooled by one of these spoofed websites, they will often input their personal and/or financial information, like a credit card or bank account number, which is directly funneled to a criminal actor who uses it to steal their money. Phishing is by far the most frequent internet crime reported to the FBI, with over 193,407 complaints received in 2024 and over $70 million in reported losses in the United States.[12]

---

[10] Santoshi Nakamoto, *Bitcoin: A Peer-To-Peer Electronic Cash System*, Bitcoin.org (Oct. 31, 2008), https://tinyurl.com/2vyrxxby.
[11] *See Transparency*, Tether.com (Oct. 7, 2025), https://tinyurl.com/2vabzysu.
[12] *See Federal Bureau of Investigation Internet Crime Annual Report 2024*, FBI Internet Crime Complaint Center (Apr. 23, 2025), https://tinyurl.com/55pwfp6a.

21. Despite the scope and reach of this crime, it is relatively easy to commit, thanks in large part to the developers of phishing software like Lighthouse. This type of software provides someone who wants to run a phishing scam with many of the tools they need to do so: templates for fake websites spoofing hundreds of well-known businesses; the ability to mass-distribute text messages; and a platform to collect and organize stolen personal financial information. For a monthly licensing fee of approximately $200, a scammer can create hundreds of websites that could reach thousands of victims. For a little extra money, scammers can request training and tutorials from the software developers, or assistance building their own custom websites, spoofing whatever business they choose. Telegram communities created and used by the software developers connect scammers with co-conspirators providing other necessary resources: data brokers who supply lists of potential victims' contact information;[13] "spammers" who specialize in strategies for sending out text messages in bulk, often operating farms of multiple cell phones or SIM cards;[14] and other specialists to help launder stolen funds once scammers acquire phished credentials.[15]

[13] Data brokers collect bulk sets of contact information from various sources including public records, social media, and data breaches. *See What to Do If a Scammer Has Your Phone Number*, Identity Guard (Feb. 14, 2020), https://tinyurl.com/2bynehp2. For example, in 2021, hackers claimed to have stolen the data of 100 million T-Mobile customers, which they sold on the dark web. Breached data is often available for sale in dark web forums relatively inexpensively. *See, e.g.*, Brian Barnett, *The T-Mobile Data Breach Is One You Can't Ignore*, WIRED (Aug. 16, 2021), https://tinyurl.com/23xwyb3p.

[14] Telegram forums sell both the hardware necessary to send these messages in bulk and access to service providers who operate the hardware on behalf of scammers. One piece of hardware used to do this is an SMS modem pool that can operate over 500 SIM cards, allowing messages to be sent in bulk from telephone numbers that appear to be coming from the United States. *See* Gary Warner, *SMS Pools and what the US Secret Service Really Found Around New York*, Security Boulevard Blog (Sept. 29, 2025), https://tinyurl.com/yta29z8e.

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

22. There is consensus among security researchers that a small number of purveyors are responsible for developing some of the most widespread phishing scams worldwide. One example is Wang Duo Yu, who claims to be the primary developer of Lighthouse. Wang Duo Yu and the other purveyors are believed to be located in China.

23. While the exact scope of the fraud connected to Lighthouse is not easily quantifiable, Lighthouse is undoubtedly one of the most pervasive phishing software products available today. Cybersecurity firm Silent Push estimated that during their research over a 20-day period, approximately 200,000 fraudulent websites created with Lighthouse were used to attract "well over 1,000,000 potential victims" in over 121 countries.[16] They also estimated that Lighthouse-supported phishing websites received an average of 50,000 page visits per day. SecAlliance, a cybersecurity firm, attributed 32,094 distinct United States Postal Service ("USPS")-themed phishing websites to Lighthouse from July 2023 through October 2024, estimating that between 12.7 million and 115 million credit cards may have been compromised in the United States alone.[17]

24. One of the most common SMS phishing scams perpetrated through Lighthouse begins with a fake USPS text message, purporting to notify a victim that they missed a package delivery. The message includes a link for the victim to reschedule their delivery. If a victim clicks the link, they are directed to a fake USPS website that requires payment of a small redelivery fee.

---

[16] *See Smishing Triad: Chinese eCrime Group Targets 121+ Countries, Intros New Banking Phishing Kit*, Silent Push Blog (Apr. 10, 2025), https://tinyurl.com/4ye8ht6d. Some security firms use the term "Smishing Triad" to refer broadly to Wang Duo Yu and other China-based phishing software developers, but Silent Push's research focused on the Lighthouse software.

[17] *See Research: The Evolution of Chinese Smishing Syndicates and Digital Wallet Fraud*, SecAlliance (Aug. 5, 2025), https://tinyurl.com/48d4vh49.

Of course, the original text message was a ruse, and there is no package to deliver. The scammers simply collect any payment information that a victim types into the website.

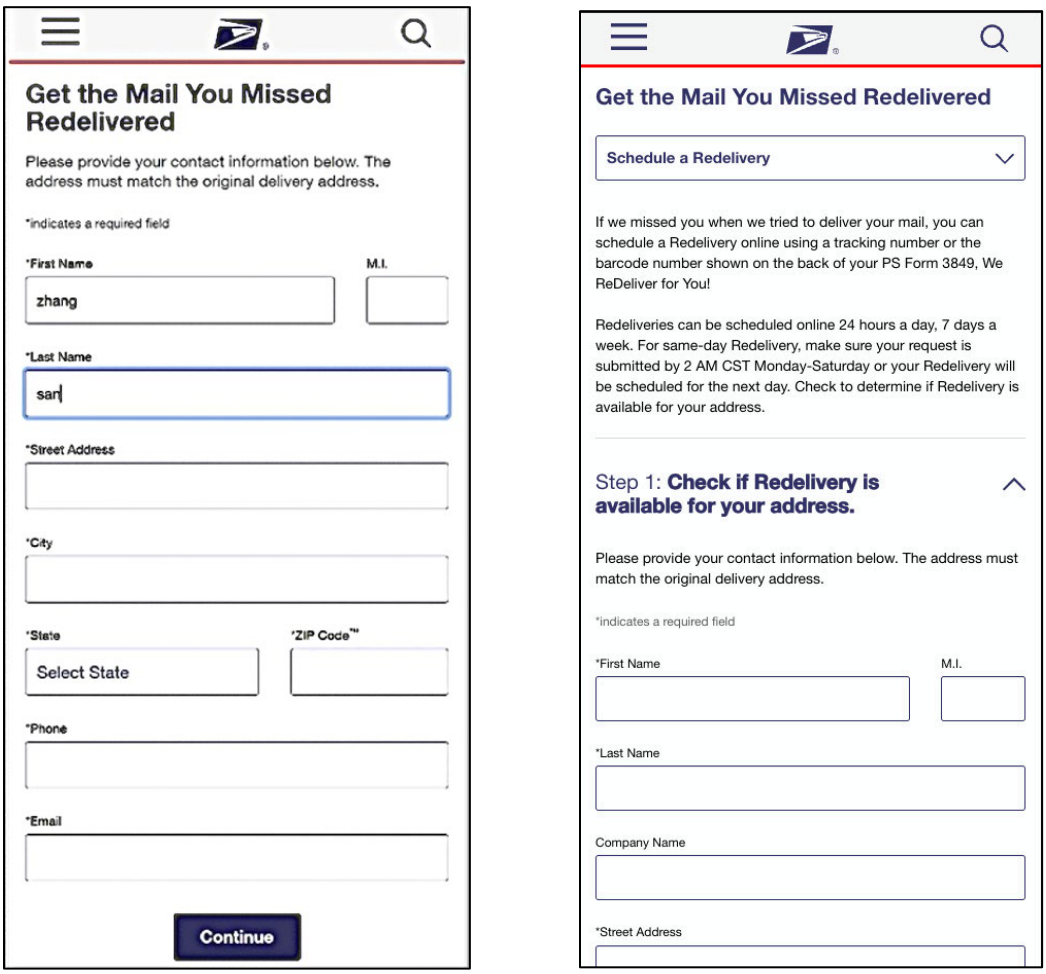


Figure 1. Screenshot from March 18, 2025, @wangduoyu0 Lighthouse Tutorial Video Showing Landing Page for Fake USPS Website, https://t[.]me/laowang_notice/4 (Left) and Legitimate USPS Website (Right) Accessed October 20, 2025

25. As discussed in more detail herein, Telegram user @wangduoyu0 claims to be a Lighthouse software developer and regularly posts public advertisements and tutorial videos on YouTube and Telegram illustrating how the software works. In one tutorial video, posted by @wangduoyu0 to Telegram on March 18, 2025, @wangduoyu0 showed the steps for using the Lighthouse software to perpetrate the USPS scam. The Lighthouse software provides a template of a fake USPS website, depicted in Figure 1. In screenshots from the tutorial video, depicted in

Figure 2, the windows to the left of the screens demonstrate the fake USPS website visible to the scam victim. Behind that window, and on the right side of the screens, is the Lighthouse software dashboard.

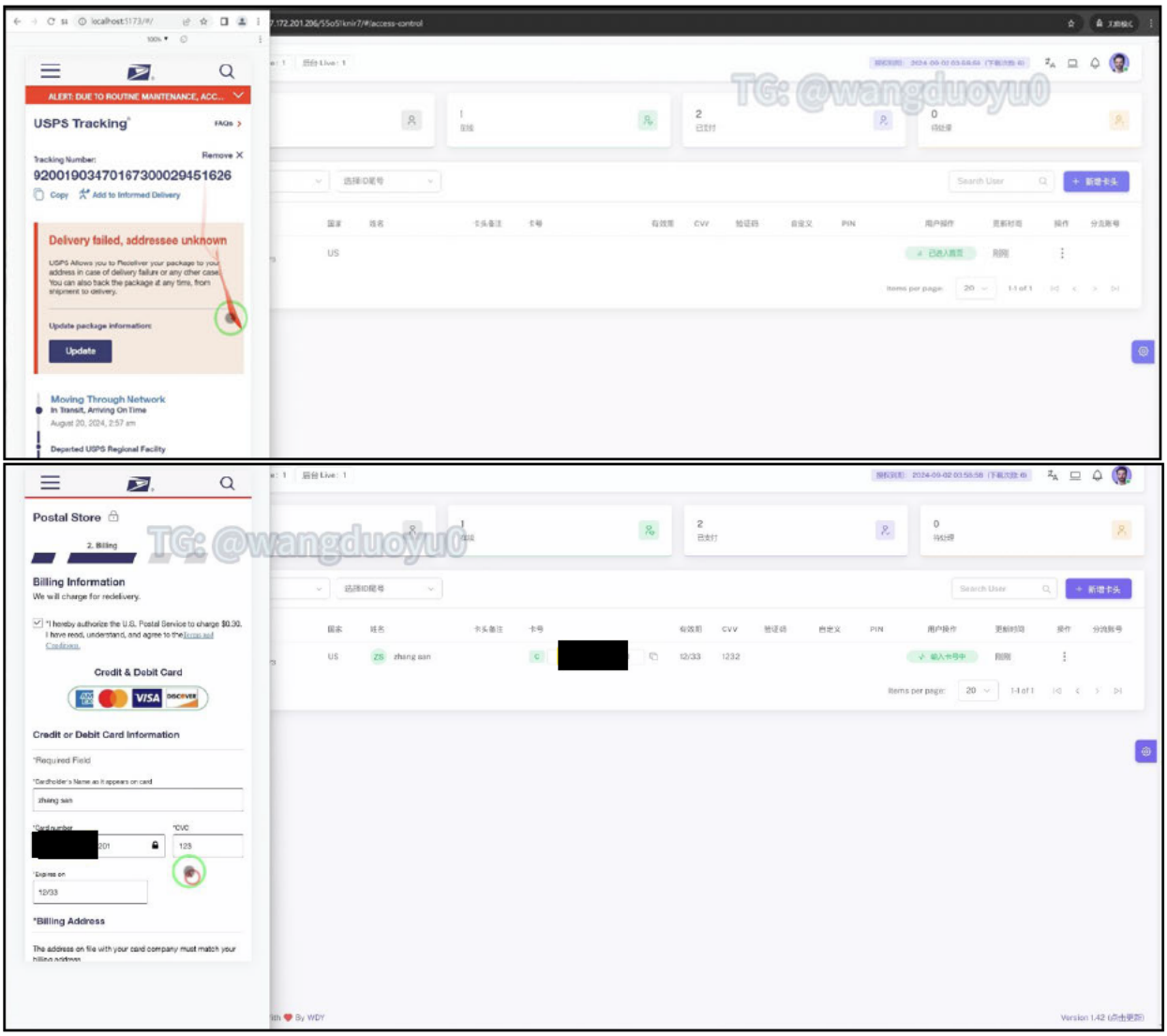


Figure 2. Screenshots from March 18, 2025, @wangduoyu0 Lighthouse Tutorial Video. https://t[.]me/laowang_notice/4 (translated)[18][19]

[18] Figures that include "(translated)" in the description have been translated from Chinese to English. At the time of my review, I used Google Translate or Telegram's translation feature. I have since had all such figures translated by a court-certified service. **Exhibit 1** includes true and correct copies of the original screenshots I took of the software, Telegram channels, or tutorial videos and the respective English translations and certificates.

[19] Ex. 1 at 7–8.

26. During the four-minute video, @wangduoyu0 showed how a potential phishing victim would input their personal information (name, address, telephone number, and email) and then be directed to a payment page that says, "[w]e will charge for redelivery." The website requests that the victim check a box saying, "I hereby authorize the U.S. Postal Service to charge $0.30. I have read, understand, and agree to the Terms and Conditions." After checking the box, the victim is directed to submit their credit or debit card information. During the video tutorial, it is apparent that as the victim types in the fake website, the information they are inputting appears in real time inside the Lighthouse interface. In the second screenshot in Figure 2, for example, as the credit card number is typed into the "Card number" box on the left, it appears next to the C icon on the Lighthouse interface. Notably, the card number appears as it is being typed, even before a victim chooses to submit the payment.

27. The USPS scam depicted in this Lighthouse tutorial video is just one simple example of the various types of frauds, some more complex, that the Lighthouse software supports. For example, the software offers templates for various toll collection scams, in which victims receive a text message purportedly from their local toll collection company, saying that they have an overdue toll bill or a fine. These scams often attempt to steal not only financial information, but driver's license information as well when a victim attempts to pay the toll.[20] Figure 3 depicts a Lighthouse template for a website spoofing New York's E-ZPass and a page stating, "your vehicle has outstanding toll invoices."

[20] Andrew Rayo, *Got a Text about Unpaid Tolls? It's Probably a Scam*, Fed. Trade Comm'n Consumer Alert (Jan. 17, 2025), https://tinyurl.com/5dyz33ta.

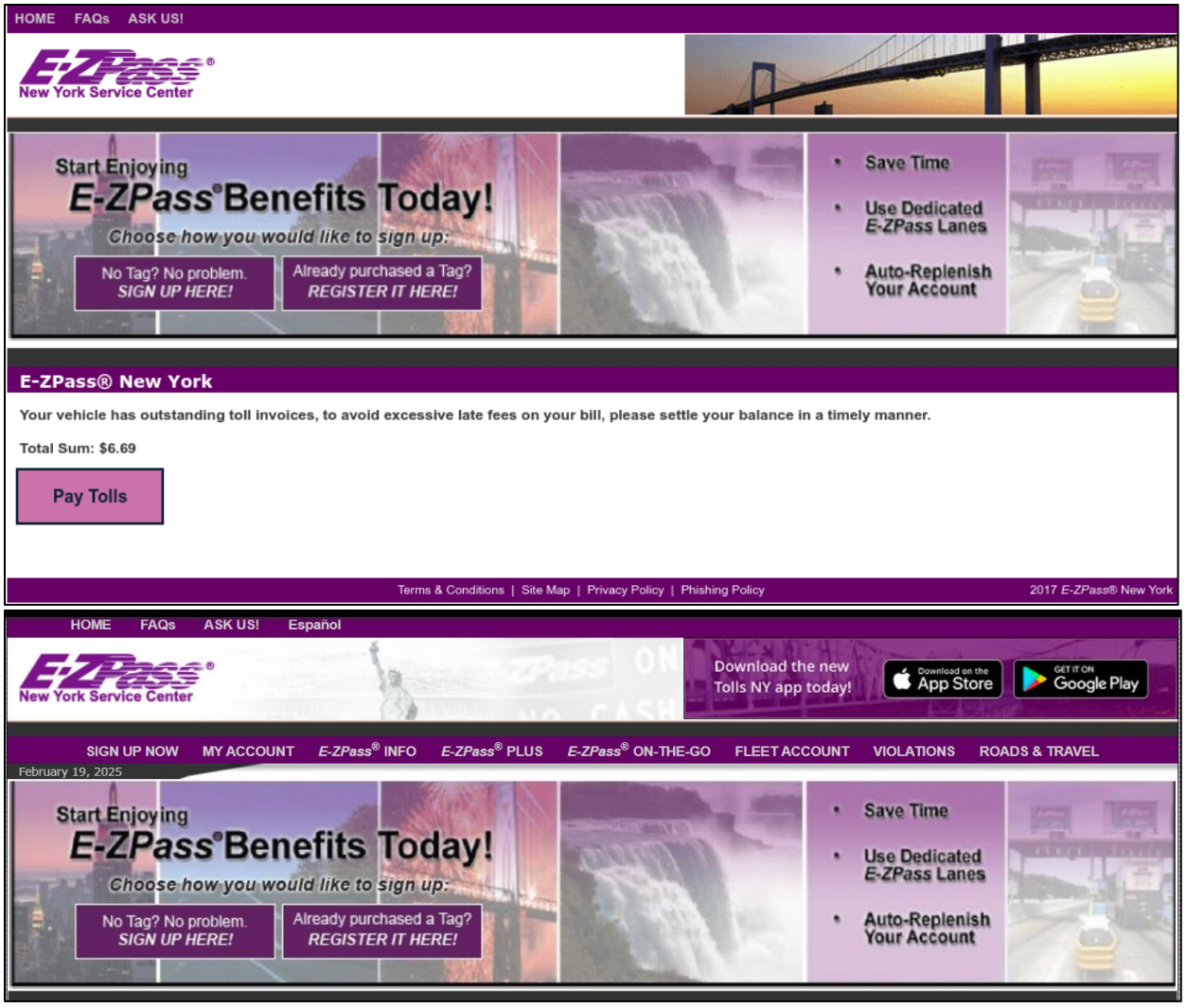


Figure 3. Template for E-ZPass SMS Scam Provided with Lighthouse Software (Top) and Legitimate New York E-ZPass Website (Bottom) as of February 19, 2025 (from Waybackmachine Internet Archive)

28. In another, similar scam, victims receive a text message stating that they have unpaid parking tickets or other motor vehicle fines. The text message includes a link to a spoof of a local department of motor vehicles or city website where victims are asked to input financial information to pay fines. The fines are bogus and the victims' financial data is stolen by the scammers.[21]

[21] *Consumers Beware! Department of Consumer Affairs Warns New Yorkers about 10 Worst Everyday Scams and How to Avoid Them*, NYC.Gov, Consumer and Worker Protection (Mar. 3, 2015), https://tinyurl.com/5d73b3db.

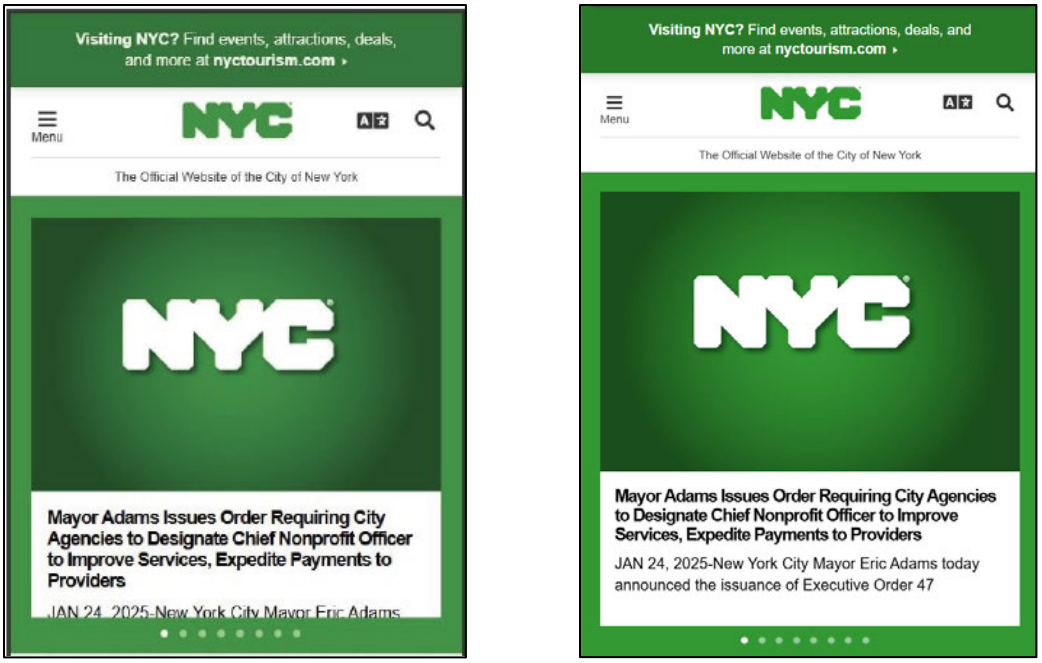


Figure 4. Template for NYC.Gov SMS Scam Posted to Telegram on January 26, 2025, https://t[.]me/dy_tongbu (Left) and Legitimate NYC.Gov Website (Right) as of January 25, 2025 (from Waybackmachine Internet Archive)

29. Lighthouse also supports various templates for SMS scams relating to financial institution accounts. In these types of scams, victims receive text messages purporting to be from their bank or brokerage company. The texts say things like, "Did you authorize this transaction?" or "Prevent your account from being frozen" or even, "You have a message" and include a link that purports to take them to the website of their financial institution. Although the victim thinks they are logging in to their financial account, they are in reality funneling their account login information directly to the scammers through the spoofed website.[22]

[22] *Stay Vigilant Against Text Scams*, Fidelity Investments Learning Center, Customer Service (Aug. 7, 2025), https://tinyurl.com/mpad6cw6.

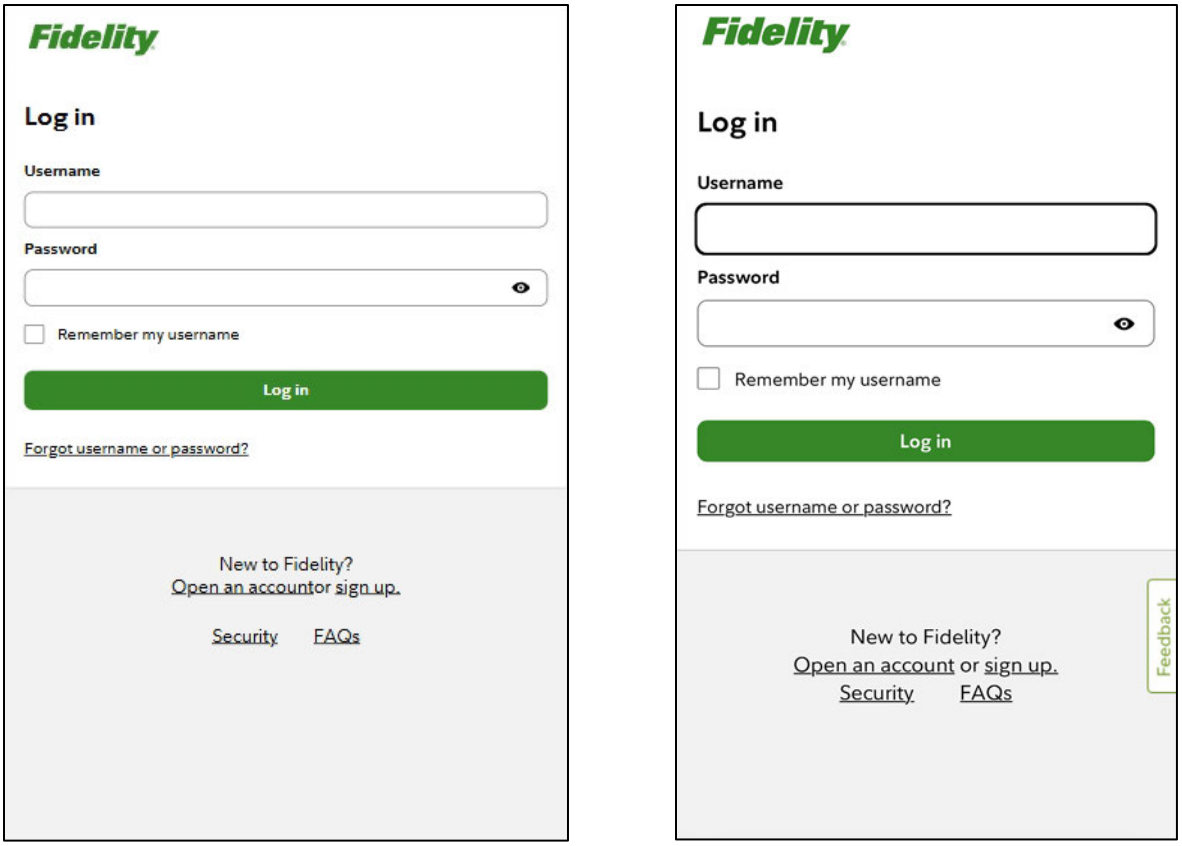


Figure 5. Template for Fidelity SMS Scam Provided with Lighthouse Software (Left) and Legitimate Fidelity Website (Right) Accessed September 25, 2025

30. The USPS, toll collection, government agency, and financial institution scams are examples of what @wangduoyu0 describes as the "SMS" version of Lighthouse. It is called the SMS version because the scams typically begin with text messages directing victims to fake websites. Lighthouse includes over 600 templates for fake websites that can be used in the SMS scam. It also supports the creation of custom campaigns, meaning that if users wanted to create a fake website spoofing a company not already included in the 600 templates, the Lighthouse software developers can work with them to do so. Lighthouse also purports to include a feature to assist the scammer in distributing mass text messages to thousands of potential victims.

31. @wangduoyu0 also offers two "e-commerce" versions of Lighthouse —one that can be used with a content management system ("CMS") platform, and another tailored to a Chinese e-commerce platform—both of which allow a user to create their own fake online store,

the only purpose of which is to steal victims' payment information. The CMS version of the tool provides scammers the ability to create a fraudulent website from scratch and integrate payment options that funnel user data to Lighthouse.[23] These pages often spoof legitimate retail websites. The Chinese e-commerce platform version of the tool supports developing a fake store on a legitimate e-commerce platform for Chinese brands. Unlike the CMS version of the software, which allows users to completely customize their website, the Chinese e-commerce platform already provides some infrastructure for an online store, and users simply add photographs and descriptions of whatever products they want to sell. Lighthouse then manipulates the payment functionality on the Chinese e-commerce platform to directly funnel any payment information to Lighthouse. In either type of e-commerce scam, when victims input personal details and payment information to purchase products on these fake websites, the information is funneled to Lighthouse and victims never receive their purchases. I believe that victims are directed to these websites through online advertisements, search results, or by accidentally mis-typing the domain of a legitimate website.

32. On April 7, 2023, @wangduoyu0 posted a tutorial video to Telegram demonstrating how to link Lighthouse to an e-commerce website. The e-commerce website used to demonstrate the functionality displayed a store called "wangduoyu" that purported to sell cell phone accessories. I note that at the bottom of the page, displayed in Figure 6, the website used in the tutorial video read, "Guaranteed Safe Checkout" and included various logos including that of Google Pay.

[23] The CMS version of the tool references a software-as-a-service company that offers tools and features that, among other things, help create websites to sell products to customers online. Its users access settings and options for their websites through a web-based dashboard that adds various functionalities and configures the user experience.

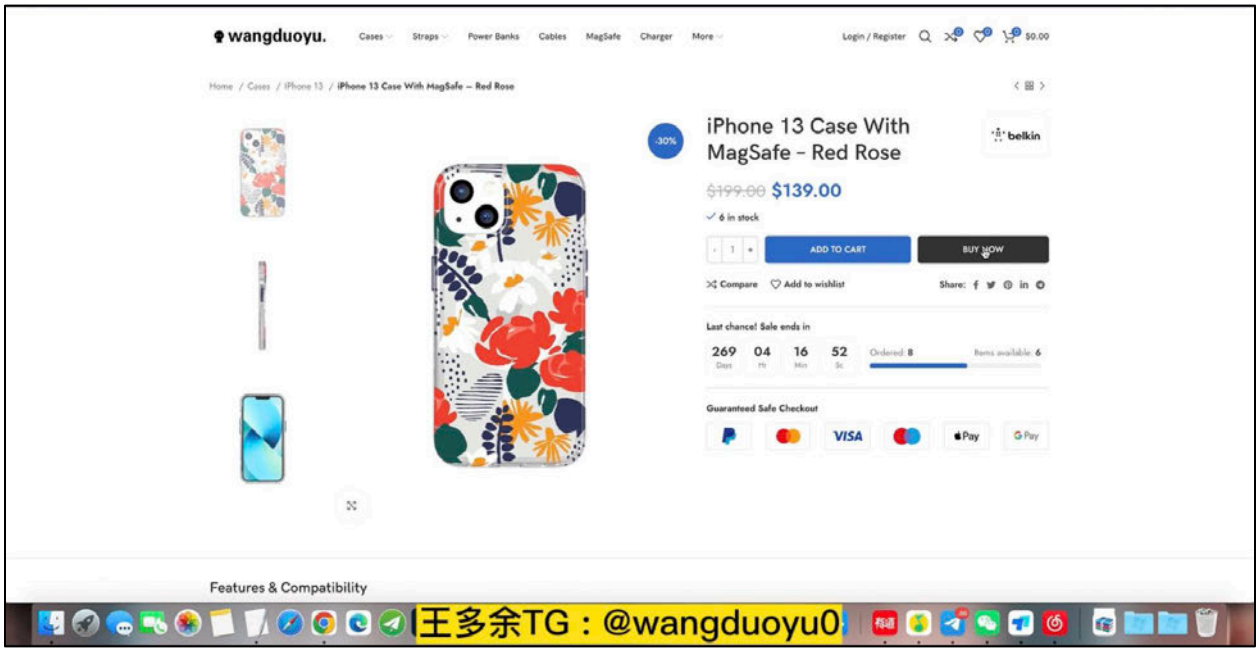


Figure 6. Screenshot from April 7, 2023, Tutorial Video Posted by @wangduoyu0, t[.]me/dy_tongbu (translated)[24]

33. As will be discussed in more detail herein, whether through an SMS or an e-commerce scam, Lighthouse also offers features to steal login information for certain online payment processing platforms, and to bypass various financial platforms' security features like MFA and 3-D Secure. It also has specific functionality that supports adding stolen credit card information to mobile wallet applications like Google Wallet.

34. Once scammers use Lighthouse to steal data, they profit from it in various ways. One common trend is to load numerous stolen credit cards onto Apple or Android mobile devices, which can be sold in bulk to criminal networks to make purchases or launder money.[25] Scam groups also have the ability to relay new stolen card information in real time to devices used by

[24] Ex. 1 at 12.
[25] *See* Brian Krebs, *How Phished Data Turns into Apple & Google Wallets*, KrebsonSecurity (Feb. 18, 2025), https://tinyurl.com/wpazfcdv.

conspirators who use them to make in-person purchases, a practice known as "ghost tapping."[26] Some recent law enforcement actions have identified networks of Chinese nationals in the United States using phones loaded with stolen credit card information using tap-to-pay functionality to purchase gift cards in bulk.[27] Other groups simply purchase their own tap-to-pay machines or rely on a mobile app that allows them to use stolen cards on tap-to-pay machines and use customer cards to make payments directly to themselves.[28] In another trend, scammers use stolen brokerage firm credentials to perpetrate a new version of a "pump and dump" scheme. In this version of the scheme, scammers pre-purchase a certain stock and then use compromised brokerage accounts to purchase large volumes of the stock, inflating the price. Once it reaches a certain price, they liquidate their original holdings.[29] Finally, phishing attacks were reported as the leading entry point for ransomware delivery in 2025 (involved in 35% of all attacks, a 10% increase from 2024),

---

[26] *See Ghost-Tapping and the Chinese Cybercriminal Retail Fraud Ecosystem*, Recorded Future (Aug. 14, 2025), https://tinyurl.com/wy5yza4c ("We believe that established, Southeast Asia-based criminal groups that have been involved in scamming activities (romance, investment scam, and cryptomining among others) since 2020 have begun and will continue to incorporate ghost-tapping campaigns into their activities for financial gains.").

[27] *See* Josh Jarnagin, *Knox County Detectives Investigating 'Ghost Tap' Credit Card Fraud*, WVLT8 (May 31, 2025), https://tinyurl.com/y2t7tvzv/; News Release, *Joint Advisory on Unauthorised Card Transactions Made Using Contactless Payment Methods in Singapore*, Monetary Auth. of Singapore (Feb. 17, 2025), https://tinyurl.com/3uabmj63 ("This modus operandi starts with the scammer … obtaining the victim's card credentials through e-commerce related phishing websites, including social media advertisements. The scammer then adds the card details onto the Apple wallet of his own device. An SMS One-Time Password (OTP) would be sent to the victim, who is then tricked to enter the OTP into the phishing website operated by the scammer, thereby giving the scammer access to their card. After successfully taking over the victim's card, the scam syndicate will conspire with a money mule to make unauthorised transactions by connecting the mule's mobile device to the scammer's Apple wallet. The money mule would then be able to make in-person purchases using the contactless payment method … to buy goods in-store, for example, high value electronic items or luxury goods.").

[28] *See* Brian Krebs, *How Phished Data Turns into Apple & Google Wallets*, KrebsonSecurity (Feb. 18, 2025), https://tinyurl.com/wpazfcdv.

[29] *See* Brian Krebs, *Mobile Phishers Target Brokerage Accounts in 'Ramp and Dump' Cashout Scheme*, KrebsonSecurity (Aug. 15, 2025), https://tinyurl.com/6z23acbu.

meaning that data collected through phishing of individuals is often then used to conduct ransomware attacks on organizations.[30]

III. Review of Lighthouse

35. As will be discussed more fully herein, Lighthouse is software that supports the creation of phishing websites, the use of those websites to steal information from victims, and the collection and organization of victim data. In order to operate, the software interacts with five sets of servers, which I will refer to as the "activation server," the "update server," the "template server," the "Lighthouse software server(s)" and the "phishing website hosting server(s)." The activation server is operated by the developers of Lighthouse and ensures that people using the software have an active license. The activation server also stores and relays information regarding the location of the update server. The update server pushes software updates to Lighthouse. The template server sends updated phishing page template files to Lighthouse. Lighthouse software servers are servers created by scammers using Lighthouse to host the software and receive stolen data from the phishing websites. Phishing website hosting servers contain the content displayed by the phishing websites. When a victim visits a phishing website, their computer interacts not only with the server hosting that website, but also directly with the Lighthouse software server, which receives the information they enter on the website. The scammer's computer, through the Lighthouse software server, receives this information in real time. A scammer using Lighthouse

[30] *See 2025 Spycloud Identity Threat Report: Trends, Benchmarks, and Strategies to Strengthen Identity Threat Protection*, SpyCloud.com (Sept. 23, 2025), https://tinyurl.com/yv9krpx3.

could have more than one of each of the Lighthouse software and phishing website hosting servers supporting their phishing operation.

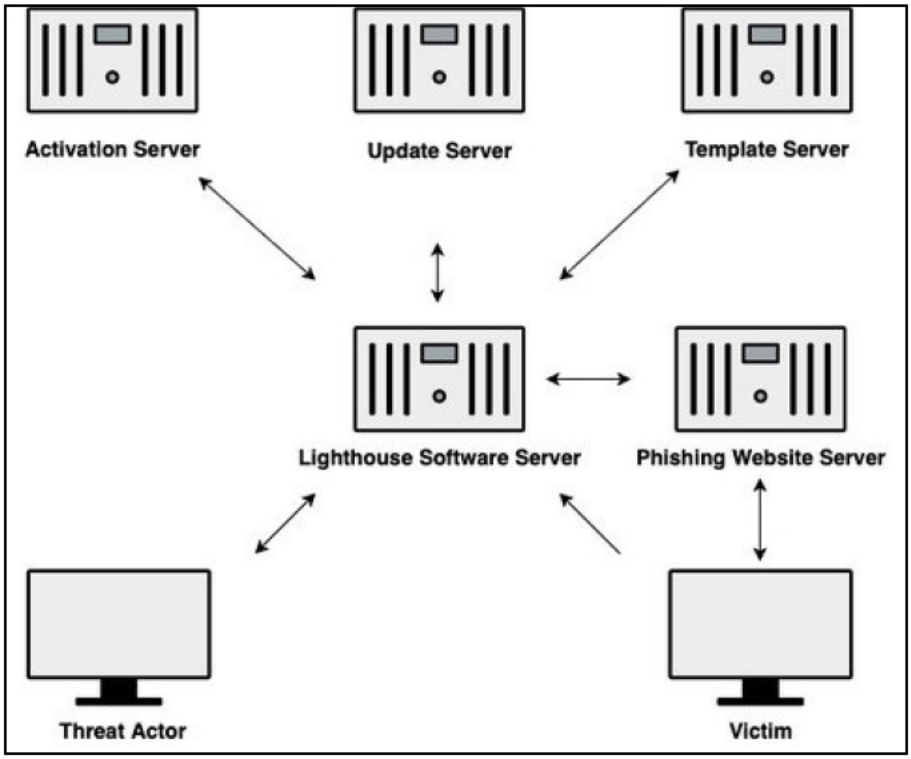


Figure 7. Servers Used to Operate Lighthouse Phishing Schemes

36. On July 30, 2025, Google provided NAXO with a copy of Lighthouse. Google acquired the software on June 2, 2025, from the official Lighthouse distribution site [redacted] which also displayed instructions to download the installation script "install.sh." The installation script "install.sh" downloaded a "setup.zip" file from the URL [redacted][1] Specifically, Google provided us with the following relevant files:

i. install.sh: Script for downloading, installing, and configuring Lighthouse and required dependencies;

[31] On September 28, 2025, a domain registration query for [redacted] indicated that the domain was registered on August 2, 2024. The domain registration for [redacted] expired on August 2, 2025.

ii. setup.zip: Lighthouse application source code and supporting configuration files downloaded by the installation script; and

iii. spider_ip.json: List of IP addresses downloaded by the installation script and used to configure firewall rules on the application server to block requests from known web crawlers.

37. I compared the hash values for the "install.sh" and "setup.zip" files downloaded by Google with the hash values of the files I used for analysis and confirmed that they are identical.[32]

38. I directed and supervised other NAXO team members in conducting a detailed forensic analysis of Lighthouse.

39. The Lighthouse application source code is primarily written in Personal Home Page: Hypertext Preprocessor ("PHP"), a widely used scripting language.[33] While the Lighthouse software incorporates several publicly available open-source PHP libraries, the Lighthouse-specific source code is obfuscated using techniques frequently used by malware to hinder reverse engineering.

40. When Lighthouse is started, a PHP extension[34] included with the Lighthouse installer reads and temporarily "de-obfuscates" the Lighthouse-specific source code before interpreting and running it. NAXO ran the software in an isolated test environment and captured a snapshot of the de-obfuscated source code for further analysis. Our test environment was also

[32] Hash values refer to the process of utilizing mathematical algorithms to assign a unique value to files or data to determine integrity. A change in the data of a file, even in the smallest increment possible, will change the resulting calculated hash value. To compare the two sets of files, I utilized both the MD5 and SHA256 hash algorithms, two widely recognized hashing methods.

[33] *See A Popular General-Purpose Scripting Language That Is Especially Suited to Web Development*, PHP.net (Oct. 9, 2025), https://tinyurl.com/z6t7eyu4.

[34] PHP "extensions" allow users of the software to augment or alter the functionality of PHP-based applications. *See Extensions*, PHP Wiki (last visited Nov. 6, 2025), https://tinyurl.com/2p9rrwn.

instrumented to record network connections created by Lighthouse during normal operation, which allowed us to identify other servers and infrastructure necessary for Lighthouse to operate.

41. Notably, in one Lighthouse source code file, "UtilBlock.php," the phishing software update process includes sending a request to URL [redacted] The [redacted] IP address in that URL is assigned to the domain [redacted] which was registered anonymously on August 30, 2023.[35] The request from Lighthouse to IP address [redacted] constitutes a connection to a command-and-control infrastructure that provides authentication and activation services, which is why I have termed this the "activation server." Lighthouse also performs a "GET" request to IP address [redacted] The activation server then returns a response that includes the current Lighthouse software distribution URL, [redacted] and "[redacted] which together make up the update server. The activation server also responded to a request for template information with an IP address of [redacted] which allowed me to identify the template server. The connection to IP address [redacted] the activation server, communicates the hostname of the update server and the IP address of the template server to the Lighthouse software, which then allows the Lighthouse software to receive updates that help users conduct phishing campaigns and avoid the most current anti-scam techniques deployed by service providers like Google.

42. On September 28, 2025, I conducted an IP address lookup for [redacted] the activation server, and [redacted] the template server. The servers are both hosted by

[35] Although the IP address remains, wangduofish[.]com is no longer an active domain.

[redacted], an Internet Service Provider ("ISP") with headquarters located at [redacted][36]

43. On September 28, 2025, I conducted a domain registration query for [redacted] the domain name representing the update server, which showed that the domain was registered on [redacted], a domain name service provider with a headquarters located at [redacted]. This domain also utilizes domain privacy services provided by [redacted] with a registered address of [redacted]. In addition, the [redacted] domain utilizes nameserver services provided by [redacted] a service provider with headquarters located at [redacted]

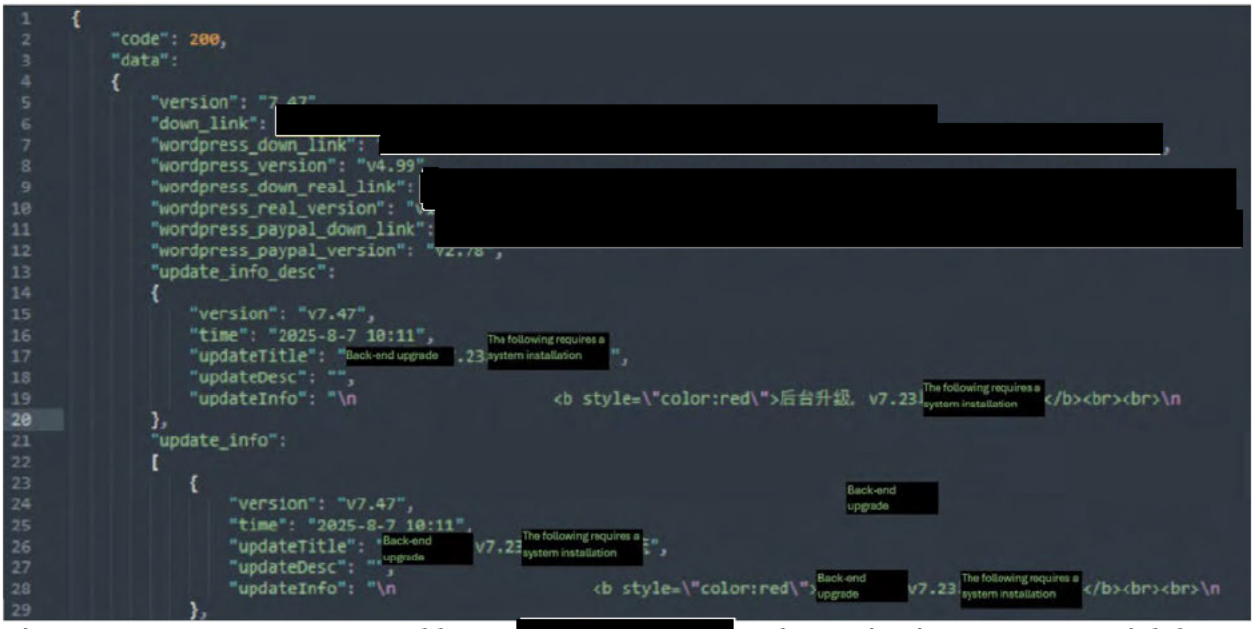


Figure 8. Response From IP Address "[redacted]," the Activation Server, to Lighthouse with Link to Update Server, [redacted] and [redacted] (translated)[37]

[36] **Appendix A** to this declaration includes the server identifiers and service providers operating the Lighthouse activation server, template server, and update server, as well as the prior Lighthouse update server, [redacted]. It also includes active domains and the registrars of each domain associated with the Lighthouse software as described further below.

[37] Exhibit 1 includes a certified translation of this Figure. Ex. 1 at 16.

44. Once I accessed the software, it opened with a login page, depicted in Figure 9. I note that the login page has icons that appear to link to Google and other platforms, but they are dead links, and nothing happened when I clicked on them.

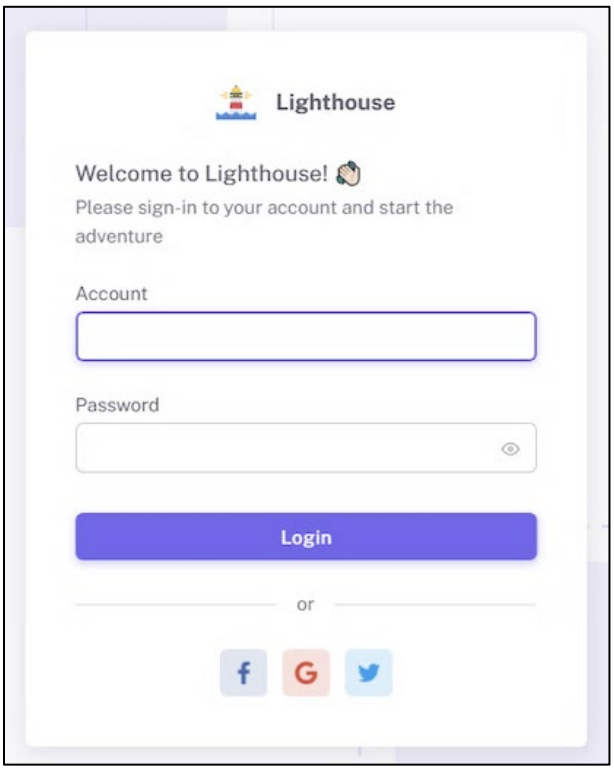
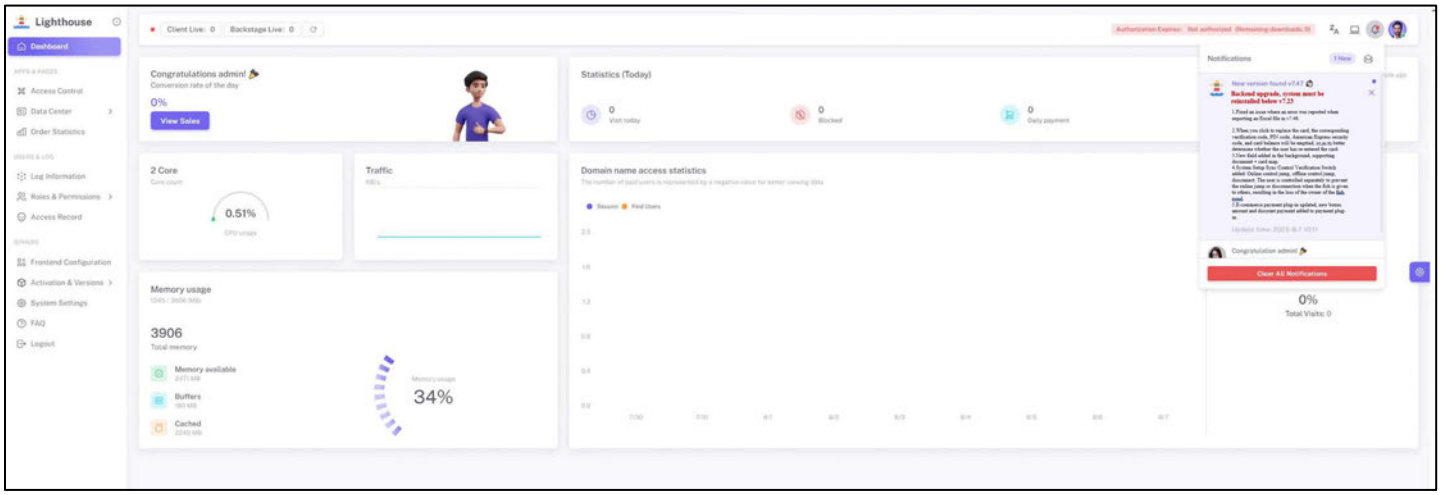


Figure 9. Lighthouse Software Login Page

45. After inputting the randomly generated account and password created when the software was installed, I observed the dashboard depicted in Figure 10.



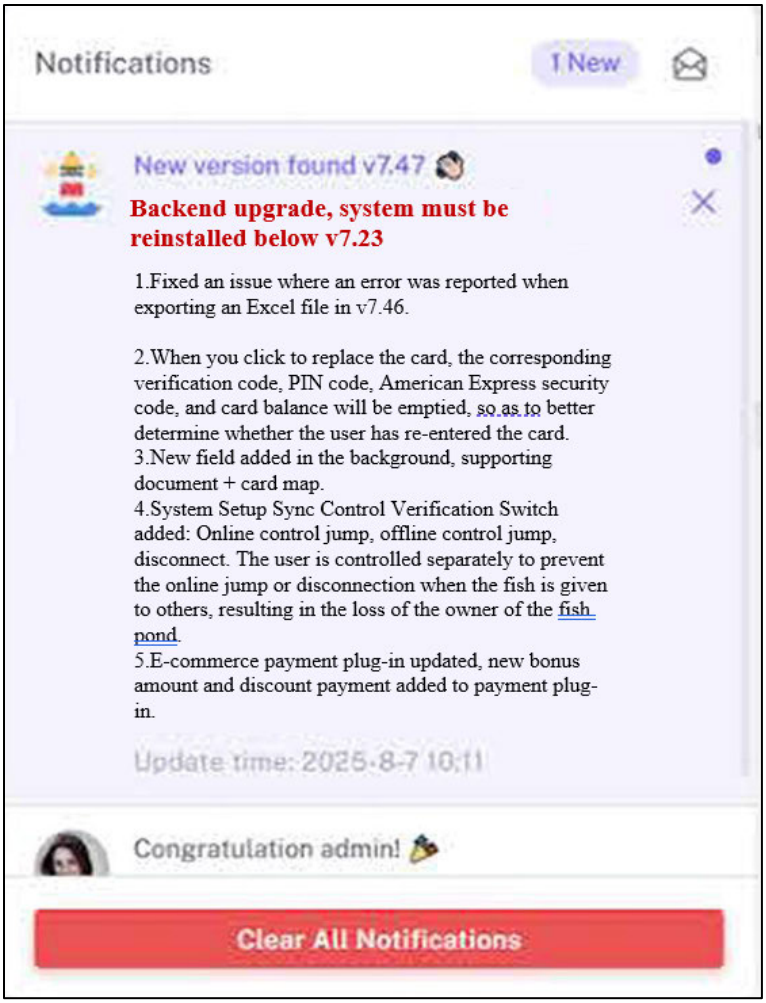


Figure 10. Lighthouse Deactivated Dashboard (translated)[38]

46. The dashboard gave me the option of choosing one of three languages: English, Chinese, and Russian. I chose English. I noted that the bottom of the page contained the following language: "© 2025, made with [heart emoji] by WDY."[39] WDY appears to stand for Wang Duo Yu. The software also indicated that this was "Backend version v7.06." I was able to review the update history from within the interface and noted that Version v7.06 was released on June 2,

[38] Ex. 1 at 20–21. The Lighthouse dashboard was in English, because I selected the English version; however, the description of software updates depicted in Figure 10 was in Chinese.
[39] Ex. 1 at 20.

2025. I noted that the June 2, 2025, release featured various updates including that "the backend uses a new architecture and the latest data encryption method, making it more secure and stable."

47. According to documentation found in Lighthouse by clicking on the "Version Update History" tab, there had been a total of 89 version updates beginning with v5.0 released on March 18, 2025, through v7.63 released on September 9, 2025, each with a description of the most recent update pushed through in a "notifications tab," in the top right corner of the home screen. Over the course of those 89 updates, the Lighthouse software added upgraded features and performance enhancements, fixed bugs, and made other adjustments to evade fraud detection practices. For example, the screenshot in Figure 10 indicated that on August 7, 2025, version 7.47 was released with various updates including, "when you click to replace the card, the corresponding verification code, PIN code, American Express security code, and card balance will be emptied, so as to better determine whether the user has re-entered the card." Tutorial videos I have reviewed indicate that the software encourages the theft of more than one type of payment information by allowing the software to tell a victim that their first method of payment malfunctioned or was declined and instructing them to input a second form of payment. I believe that this update may refer to a way to make that process easier for the Lighthouse user. For another update, labeled v7.45, released on July 26, 2025, the description read, "E-commerce payment plugin v10.10 update, changes to data transmission encryption to prevent security detection, and fixes balance query." I understand that credit card processors, security researchers, and law enforcement agencies are continuously utilizing tools and techniques to identify fraud and scams. The v7.45 update to Lighthouse appeared to alter encryption techniques in an attempt to evade detection by these groups. In a separate update, the description included, "prevent[ing] some mobile browsers from detecting suspicious activity," which I also understand to refer to evading

the fraud detection practices of ISPs. While the software was not automatically updating, it was clearly connected to the update server, which continued to push notification of available updates to Lighthouse users. I also noted that in red at the top of the home page, depicted in Figure 10, there was a warning stating, "Activation Expires: Not authorized (Remaining downloads 0)." I learned that in order to use the software, I would need a license, referred to as an "activation code."

48. I clicked through the various pages in the dashboard. Clicking on the "Data Center" dropdown menu and selecting the "All" tab displays a page for reviewing information collected from one or more phishing campaigns controlled by Lighthouse. Columns include name, payment, status, IP, and created time. A search filter allows the user to sort data by domain, date, card number, and payment status. Figure 11 depicts a screenshot of the Lighthouse "Data Center."

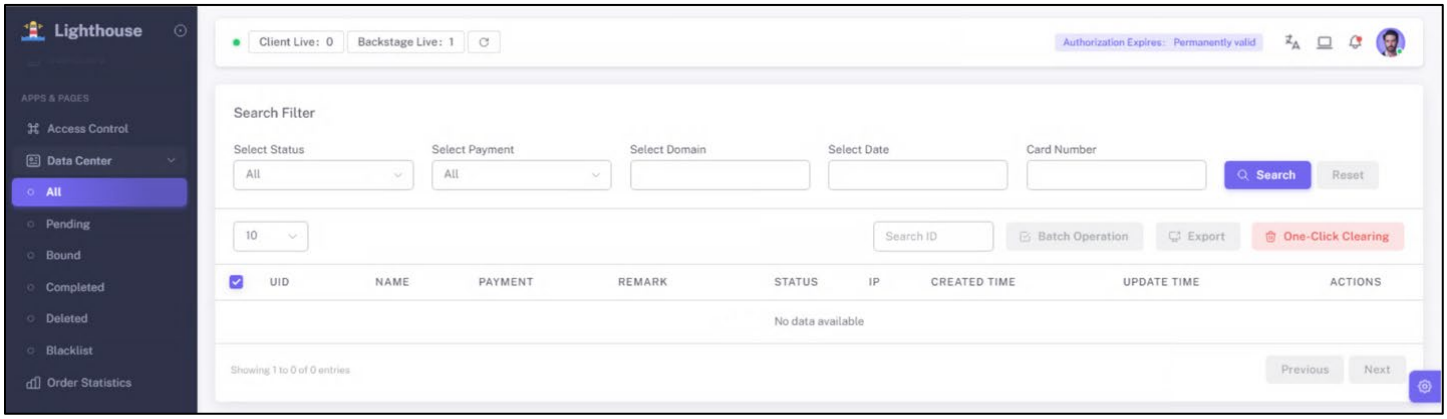


Figure 11. Lighthouse Data Center

49. Another dashboard option read, "Frontend Configuration." Based on my knowledge of Lighthouse and the video tutorials posted by @wangduoyu0 to Telegram, I understand that "Frontend" refers to the fraudulent webpage displayed to phishing victims. As I had not downloaded any code, it read "empty."

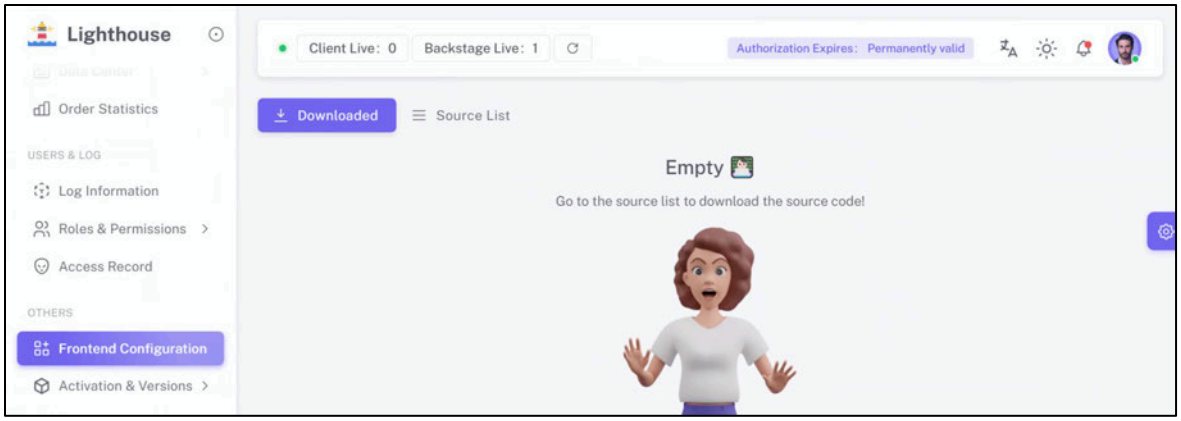


Figure 12. Lighthouse Empty Frontend Configuration

50. On the "source list," however, I was able to review over 600 templates of phishing websites. The list was sortable by area, country, official website, and update time. The official website is the legitimate website of the entity being spoofed by the phishing template. Each template also included a thumbnail image described as a "site preview." One of the templates was for an e-commerce scam, but the others were all meant to support SMS scams, meaning that they were templates for websites that would be visited after a potential victim clicked a link sent by messaging systems such as text messages, RCS, or iMessage.

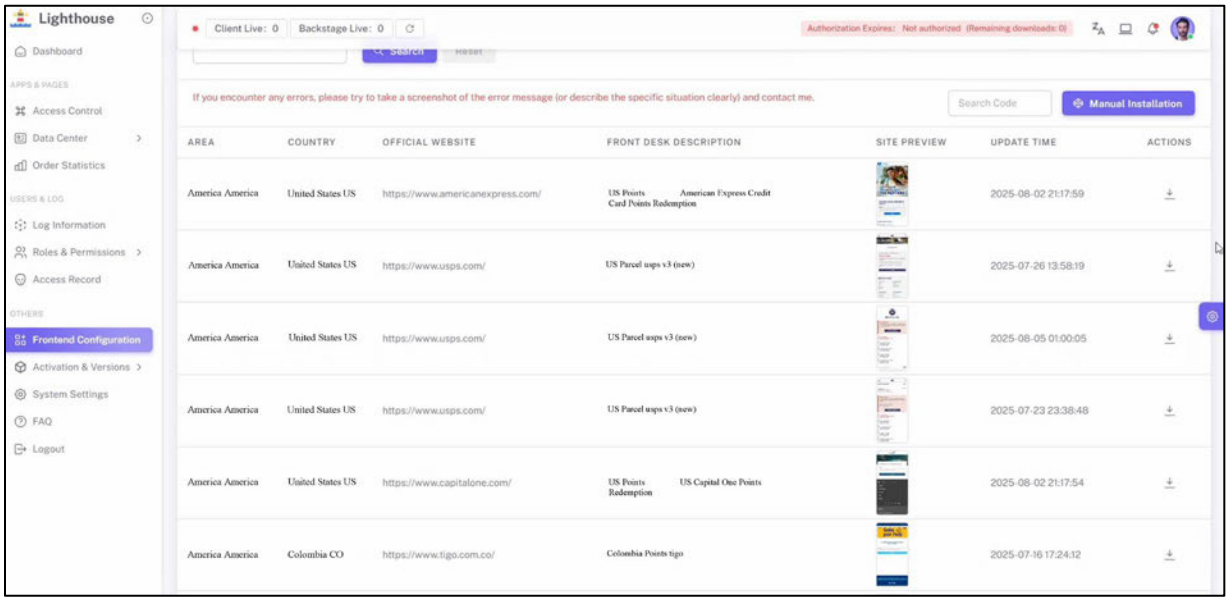


Figure 13. Lighthouse Frontend Configuration SMS Website Templates (translated)[40]

[40] *See* Ex. 1 at 25.

51. Clicking on the thumbnail image showed what appeared to be a login page for each phishing website template. Figure 14 shows an example of a thumbnail image purporting to be the login page for a food delivery company. Various of these thumbnail images appear to have a link with Google's logo. For example, the login page in Figure 14 also says, "[c]ontinue with Google." As this is simply a thumbnail image of the purported login screen, I do not know what happens when someone clicks on that link in a live page.

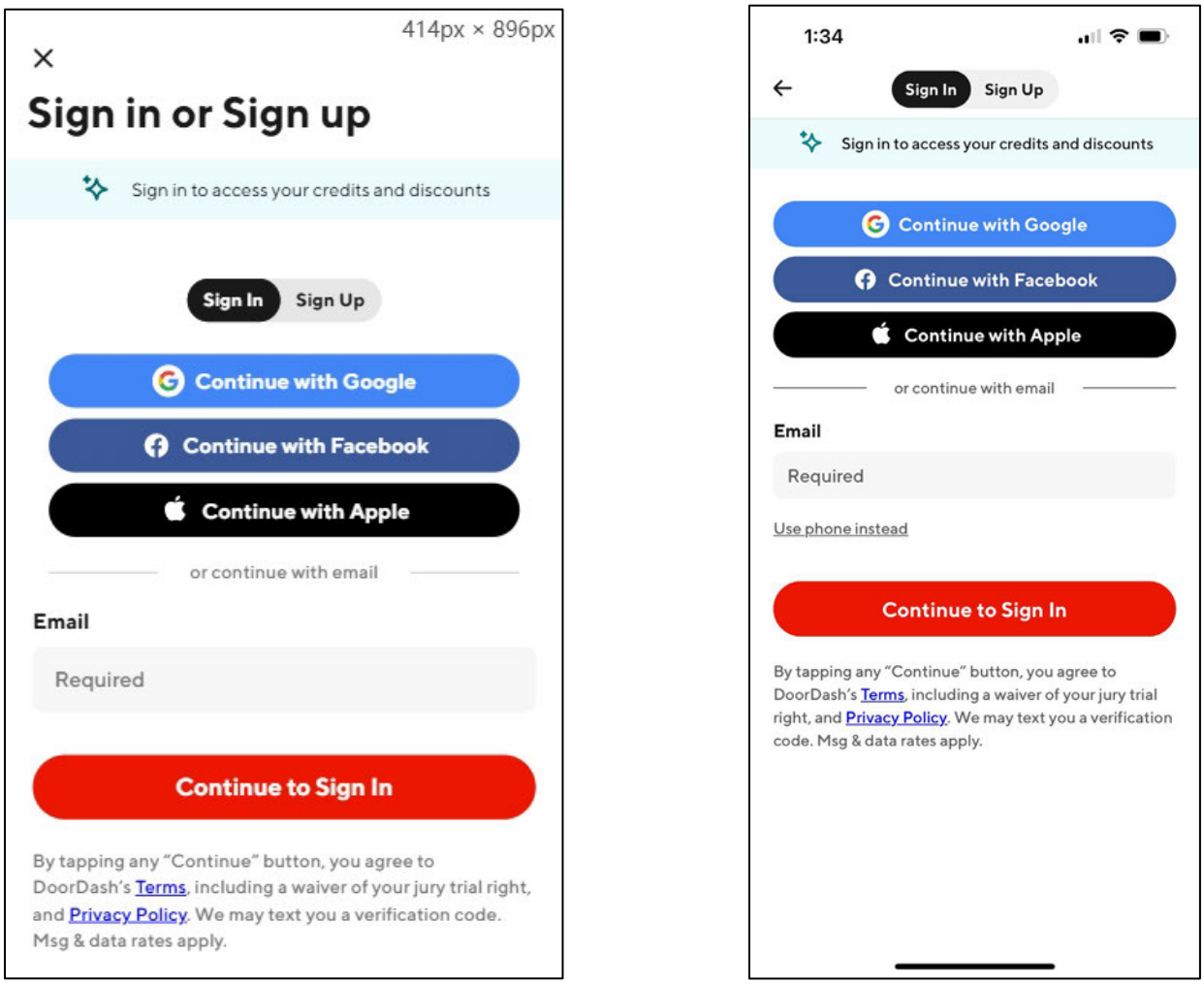


Figure 14. Example Frontend Configuration Template from Lighthouse (Left) and Legitimate DoorDash Mobile Login Accessed September 25, 2025 (Right)

52. NAXO team members reviewed all of the templates available in the software. The templates spoof over 400 distinct entities. Of those, 197 were categorized by Lighthouse as targeting the United States—the largest number targeting any single country, as reflected in the graphic below. Of the phishing templates categorized in the software as targeting U.S. victims, 73 were toll collection websites, 22 were financial institution websites, 19 were government websites, three were shipping company websites (including USPS), and two were online retail websites. Two of the templates spoofed nyc.gov and e-zpassny.com, specifically targeting victims in New York. The software included templates targeting over 120 other countries, as well as one spoof of a shipping company that did not specify a target country.[41]

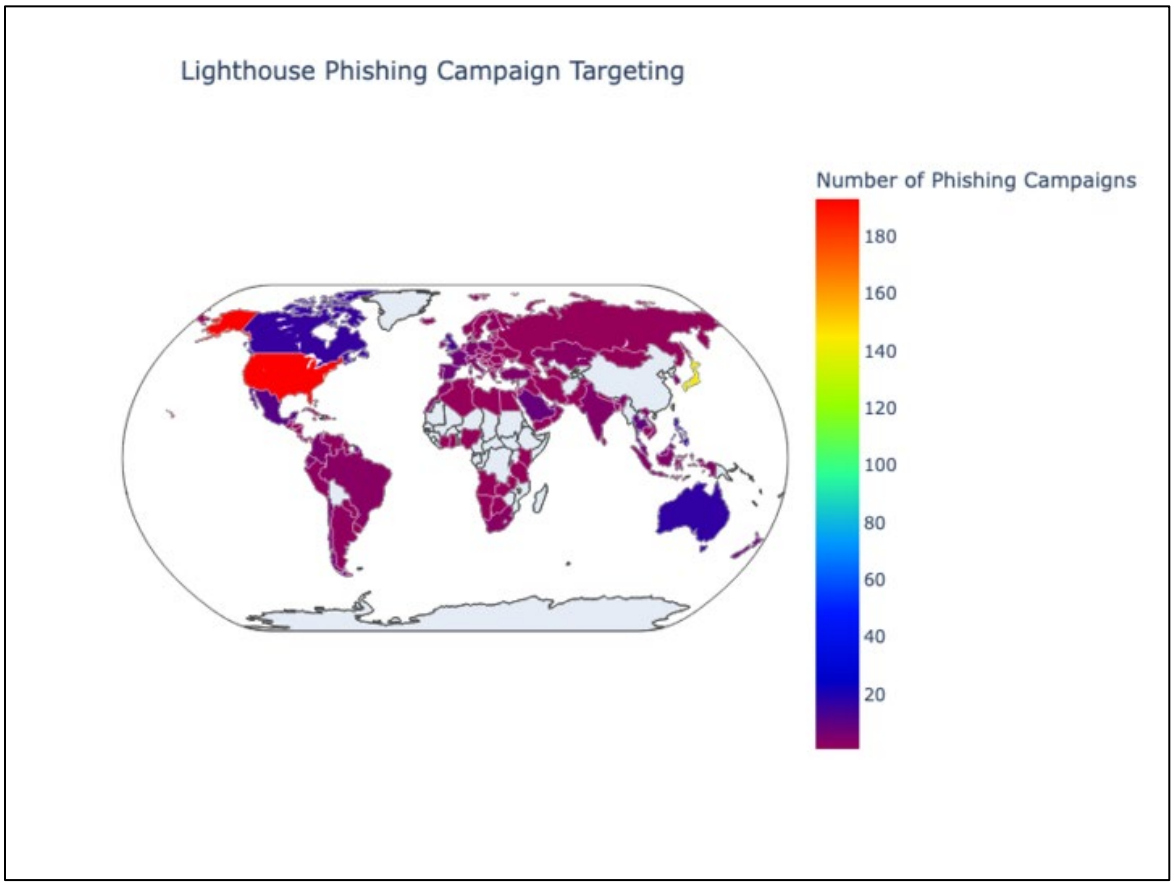
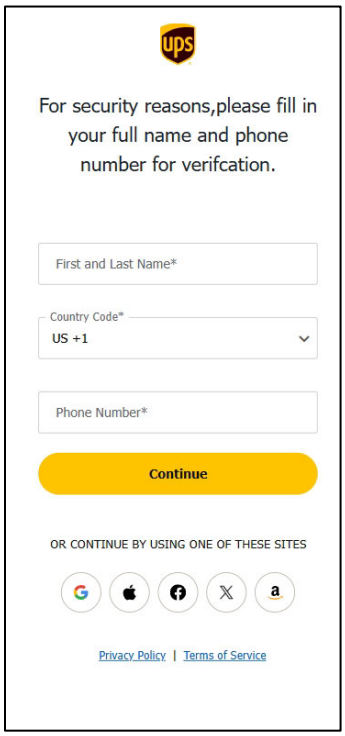
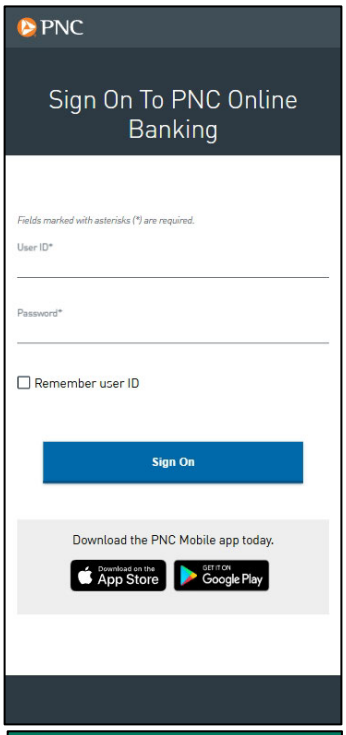


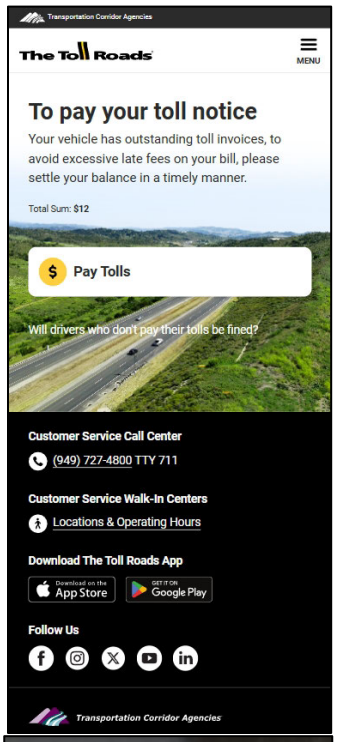
Figure 15. Map of Countries Targeted by Lighthouse Phishing Templates by Volume

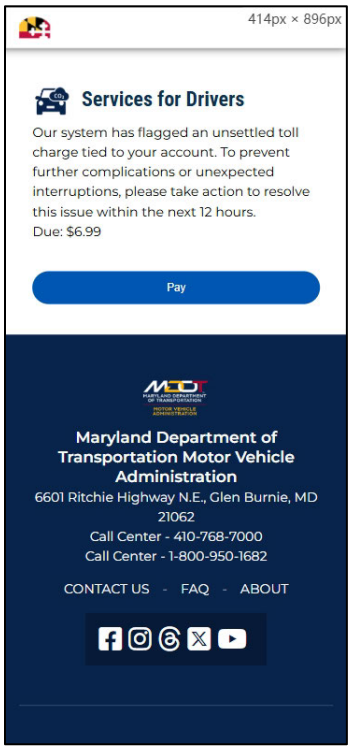
[41] Although the templates are categorized within Lighthouse based on target country (as they are typically modeled on the way a spoofed website looks to customers in that country), there is no technical limitation preventing them from being used to target victims in other countries.

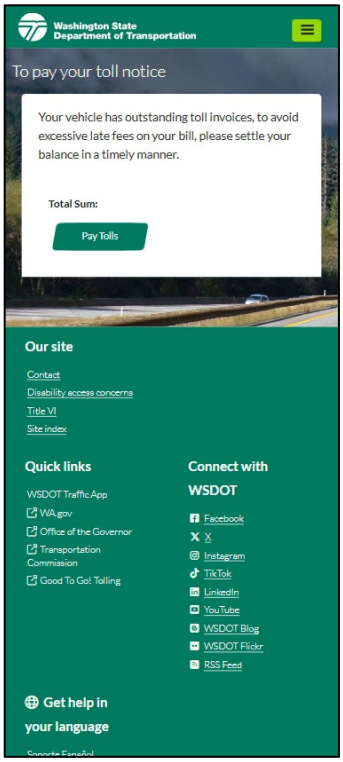
53. One hundred and sixteen of the templates include a Google logo (YouTube, Gmail, Google, or Google Play) on the login screen. Examples of templates displaying each of these logos are included herein:

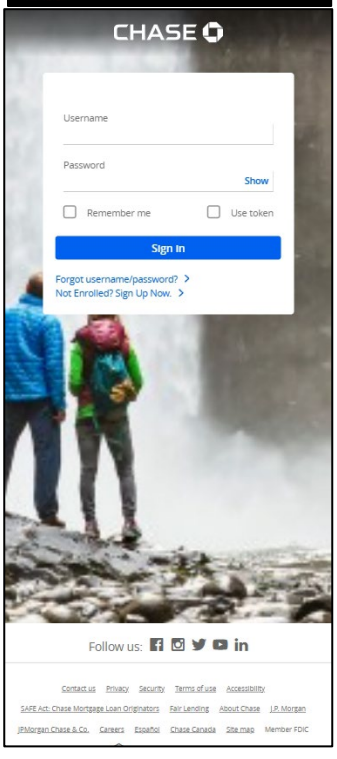


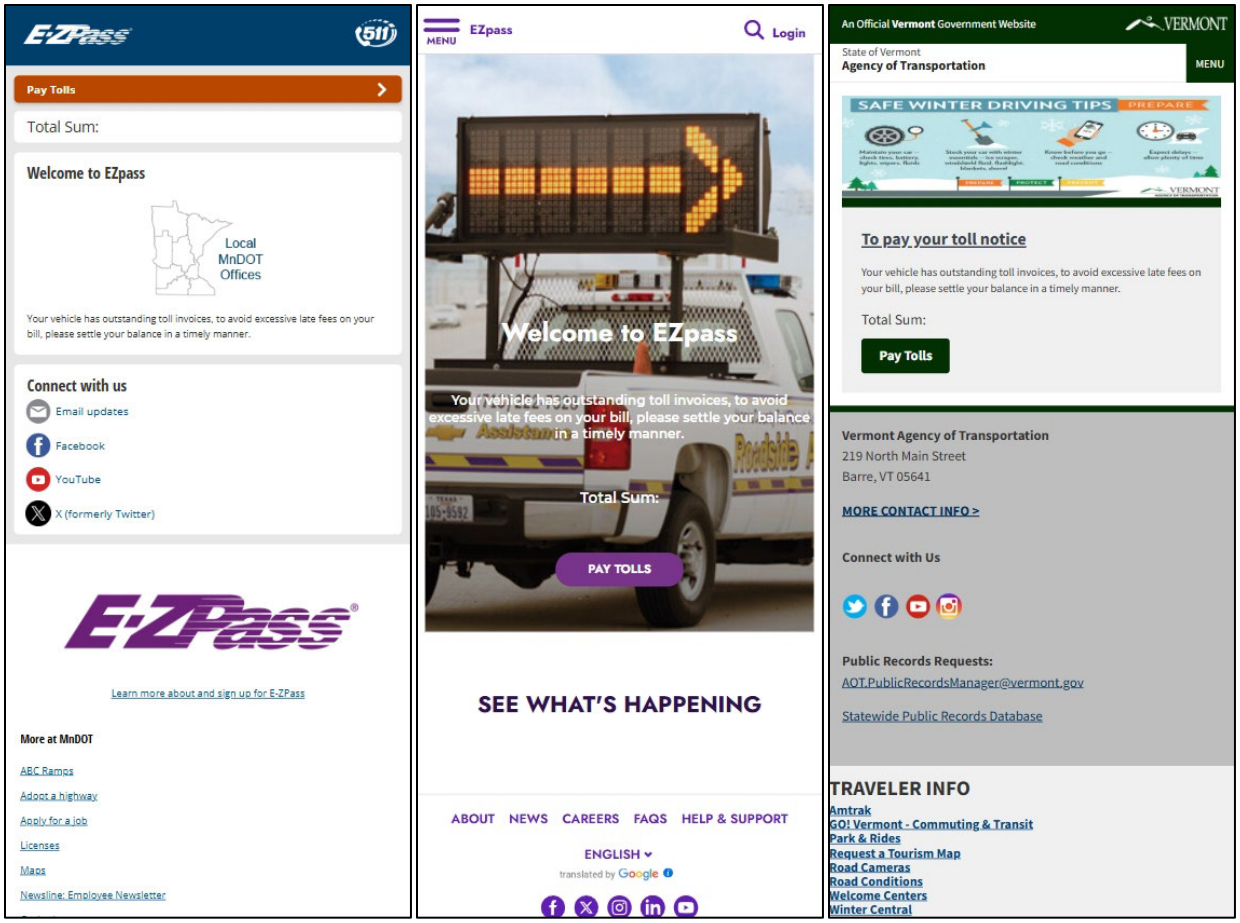












54. Although I was initially unable to download any of the templates without a license, I noted that Lighthouse remained in communication with the update server, which provides template updates, because the number of templates increased over time. For example, from August 6, 2025, to November 4, 2025, the number of available templates increased from 614 to 690. **Appendix B** is a true and correct list of Lighthouse templates with screenshots of each template as of November 4, 2025.

55. The next step in our analysis was to bypass the software's license activation requirement so that we could view and interact with the platform from the perspective of a typical paid user. We used publicly available network diagnostic tools to record and analyze computer network traffic sent automatically between Lighthouse running on our computer and the activation

server, which appears to be used to validate activation codes. We determined that Lighthouse self-reports the IP address of the server on which it is running (the Lighthouse software server) to the activation server to determine if that IP address is associated with a valid activation code, but the activation server does not actually validate that the Lighthouse software server's self-reported IP address is correct. In other words, an unlicensed Lighthouse software server can "pretend" to be a licensed Lighthouse software server by self-reporting the licensed Lighthouse software server's IP address.

56. We identified the IP address of an active Lighthouse software server based on a tutorial video posted by @wangduoyu0. After updating our server to report the IP address of that active Lighthouse software server, Lighthouse displayed a notification in the upper right-hand corner of the platform stating, "Authentication Expires: Permanently valid." Clicking on the "Dashboard" tab in the upper left-hand corner displayed a series of boxes including information on traffic bandwidth, memory usage, domain name access statistics, orders, and payments. Figure 16 depicts a screenshot of the activated Lighthouse dashboard.

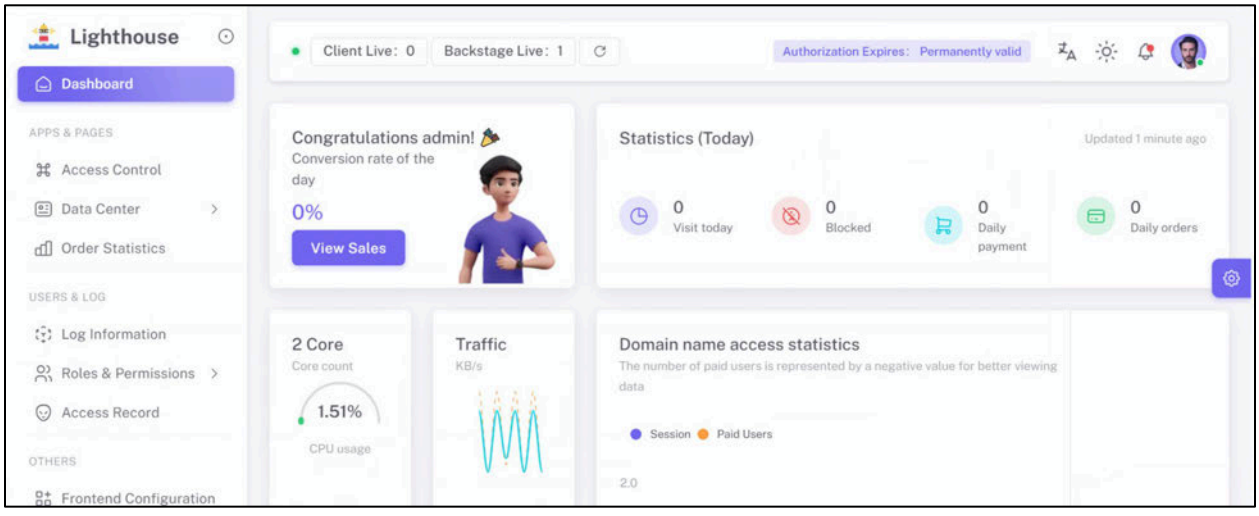


Figure 16. Activated Lighthouse Dashboard

57. This time, when I navigated to "Frontend Configuration," I noted that it was no longer "empty" but populated with something that translates to "E-commerce WordPress Stripe

Global" (hereafter referred to as the "CMS Template"). As I came to learn, the version of the Lighthouse license that I activated was the license supporting the CMS e-commerce version of the software.[42] Figure 17 depicts a screenshot of the Lighthouse "Frontend Configuration" page with an activated license.

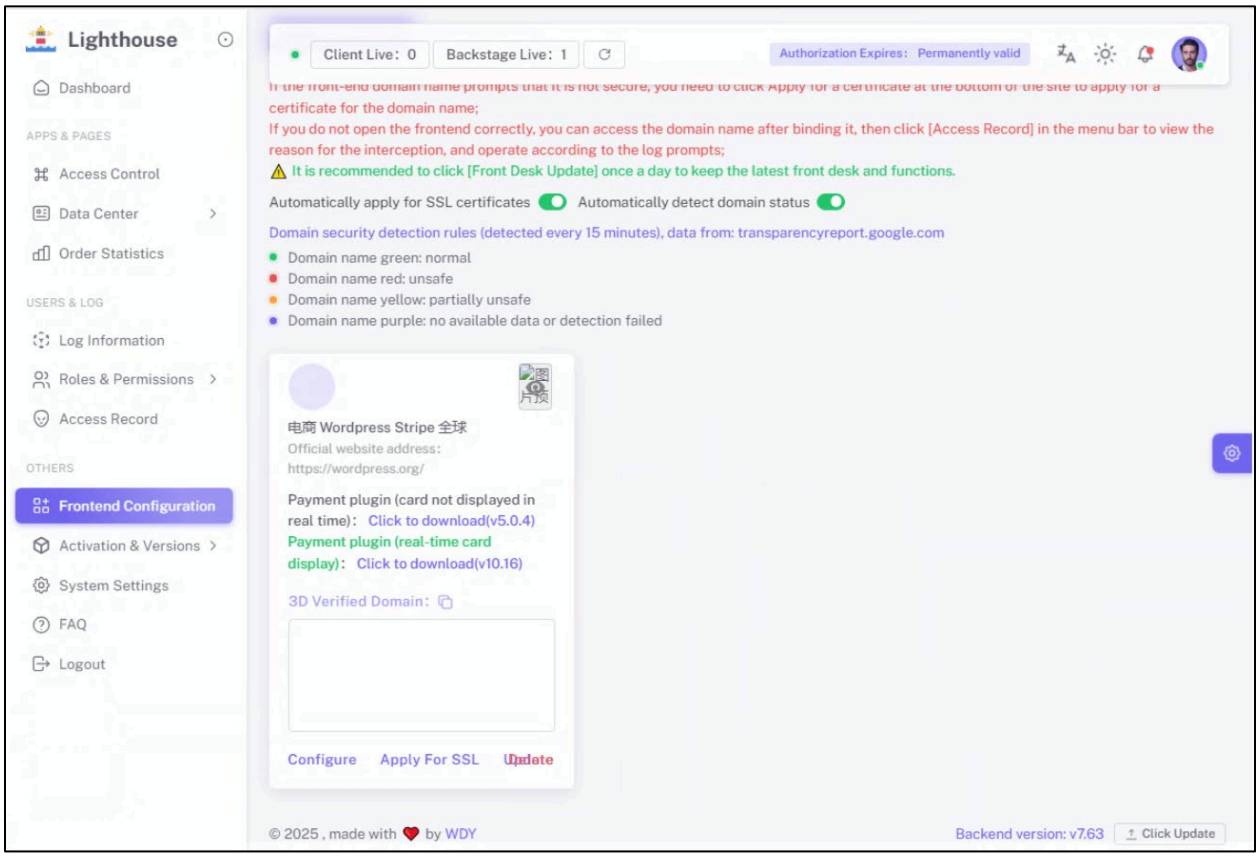


Figure 17. Frontend Configuration Activated with the CMS Template (translated)[43]

58. The CMS platform is a publicly available, full-featured platform and service for creating, deploying, and managing websites. It is modular, allowing the owner of a website to add or remove features depending on the needs of the site. This modularity is accomplished by using

[42] As will be discussed in more detail herein, although there is only one version of Lighthouse, users can purchase different types of licenses that offer features supporting different types of phishing scams. If I had an activated SMS phishing license, I believe that this page would show any SMS campaigns that I had activated.
[43] Ex. 1 at 29.

"plugins" that are selections of code, either written by application developers or by individuals, designed to implement specific functionality. For example, adding e-commerce features like the ability to add products to a shopping cart or accept various forms of payment, can be accomplished by using a plugin like "WooCommerce."[44] If the site owner wants to add the ability to accept credit card payments to their site, an additional plugin is implemented for a card processing service such as "Stripe."[45]

59. The box containing information pertaining to the CMS Template included links to download two "Payment Plugins." The first reads, "Payment plugin (card not displayed in real time): Click to download (v5.03)" and the second reads, "Payment plugin (real-time card display): Click to download (v10.15)." These plugins are designed to be installed within an e-commerce website to allow Lighthouse to collect payment information from scam victims.

60. Clicking on each of the links for the plugins downloads two distinct files: "lighthouse-stripe-gateway-v5.03.zip" and "lighthouse-stripe-gateway-v10.15.zip," respectively.[46] The "Lighthouse Stripe Gateway" CMS plugin disguises itself as a legitimate card processing service, going so far as to include the term "Stripe" in the naming convention. However, when this plugin is connected to an e-commerce website, any credit card information typed into the website is directed not to an actual credit card processor, but instead directly to the Lighthouse platform. As such, the "Lighthouse Stripe Gateway" CMS plugin is unique to websites funneling data to the Lighthouse platform. Each zip file contains a similar file and folder structure with a

[44] WooCommerce is an "open-source commerce solution built on [the CMS]" that claims to "empower[] small and medium businesses to sell online by building exactly the store they want." *About Woo*, Woo (last visited Nov. 6, 2025), https://tinyurl.com/5x9ckd7j.
[45] Stripe is a platform that provides tools for business to process online payments. *Enterprise*, Stripe (last visited Nov. 6, 2025), https://tinyurl.com/2w5br34j.
[46] A zip file is a compressed container that bundles one or more files or folders.

"lighthouse-stripe-gateway" PHP file, and a folder labeled "assets." Inside the "lighthouse-stripe-gateway-v10.15.zip" "assets" folder are 19 files, some of which are image files labeled with different financial institution names. Each of these files contains an image with the logo of that financial institution. Figure 18 shows the files within the "assets" folder and a preview image of one of the logos. These logos are used by Lighthouse to create legitimate-seeming payment processing pages.

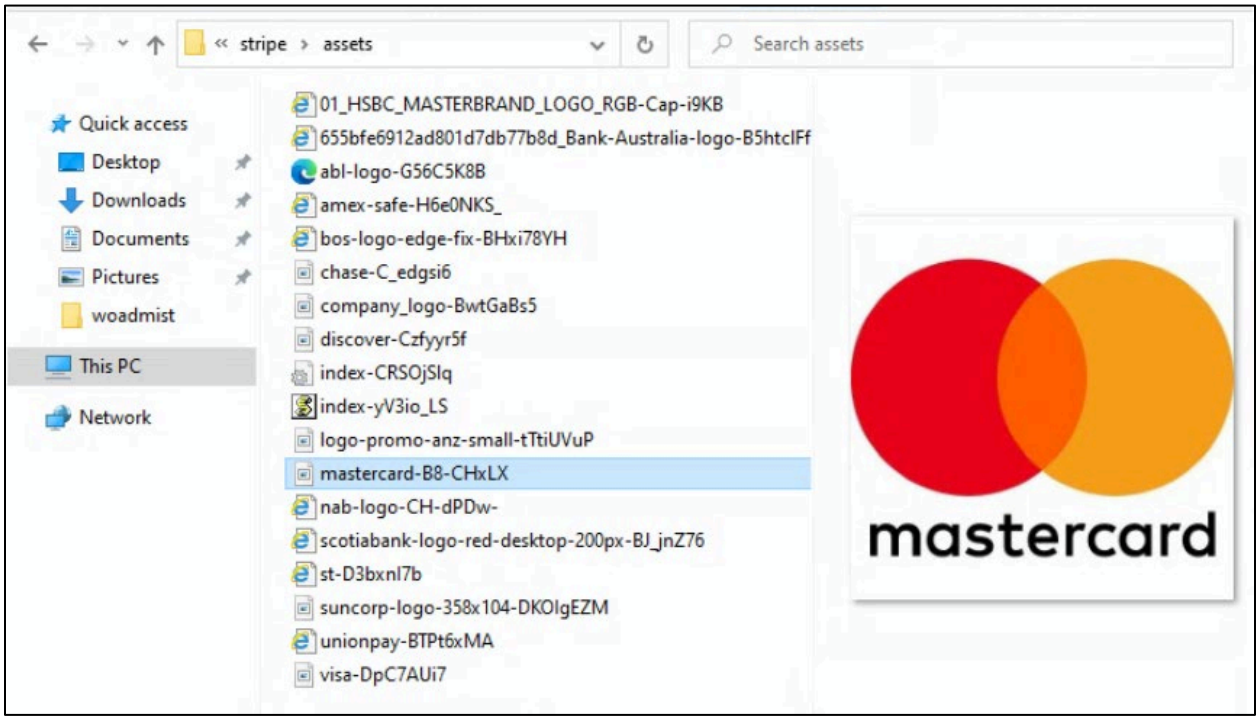


Figure 18. Lighthouse-Stripe-Gateway Download

61. Utilizing software that monitors the network traffic that is sent and received by my computer, I repeated the process of downloading one of the CMS plugins by clicking a link on the CMS Template. Reviewing the logs created during this process, I identified the download request sent from my computer to the Lighthouse update server as "GET/api/adminUser/downWordpressPlugin?coding=wordpress&requestTime=1755876298HTTP/1.1." The Lighthouse update server responded, acknowledging the request for the plugin file.

Following the acknowledgements, the network traffic logs show that my computer performed a DNS query for [redacted]

62. Clicking on the "Configure" link in the bottom left corner of the CMS Template takes the Lighthouse user through a three-step process for setting up an e-commerce phishing scam. The first step of the process is called "Domain Management" and provides a text box for the Lighthouse user to enter domain names to be configured as phishing websites.[47] A second text box labeled as "Frontend entrance" is configured by the Lighthouse user as the 3D-Secure authentication page where the phishing victim would be tricked into entering their MFA code. Figure 19 shows the first step of the Lighthouse "Frontend Configuration" process.

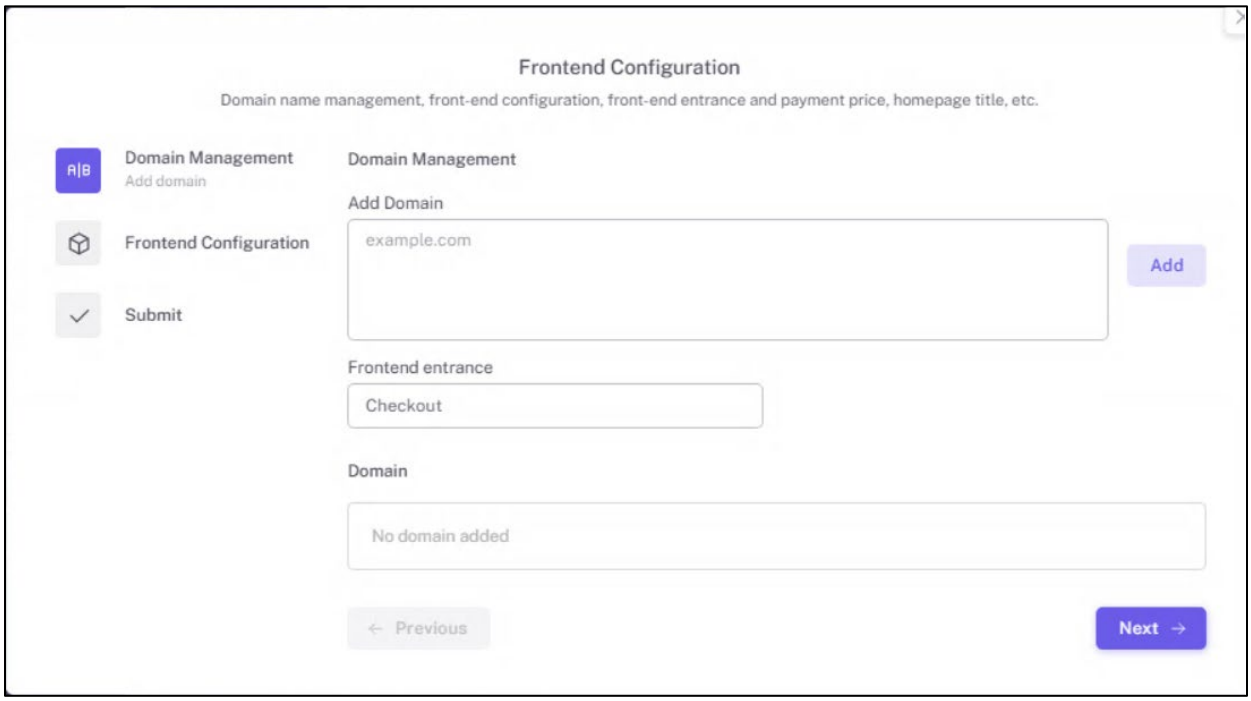


Figure 19. Lighthouse Frontend Configuration – Domain Management

63. Clicking the "Next" button brings the user to another page, entitled "Frontend Configuration," with options to limit the types of devices that can access the fraudulent phishing

[47] Although the software provides most of the infrastructure for the phishing scam, the scammers need to independently register domain names.

site. Forcing victims to access the phishing sites from mobile devices (by blocking PC access) makes it easier to trick them into entering legitimate MFA codes received via SMS into the phishing sites and may also aim to limit security researchers and law enforcement from analyzing the websites. This step includes options for blocking Apple iOS devices and Google Android devices as well, meaning that a Lighthouse user could prevent victims using one of those types of devices from accessing their phishing websites.

64. This step also includes the option to use "ipregistry anti-red API." This allows options for detecting proxy IP addresses, anonymous IP addresses, high-risk IP addresses, and others. I believe that "anti-red" refers to the red color that browsers such as Google Chrome use to mark certain websites as unsafe. Figure 20 depicts a "red" webpage flagged by Chrome. If a website is marked as potentially malicious, it makes it more difficult for scammers to convince victims to provide information to the website.[48]

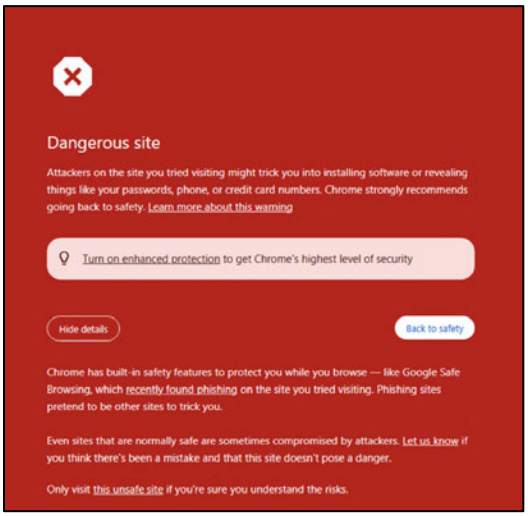


Figure 20. Example of Google Chrome Flagging "Dangerous" Phishing Website

[48] Devdatta Akhawe, *Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness*, 22nd USENIX Security Symposium (Aug. 14, 2013), available at https://tinyurl.com/4hvc7nu6 ("During our field study, users continued through … a quarter of Google Chrome's malware and phishing warnings … . This demonstrates that security warnings can be effective in practice; security experts and system architects should not dismiss the goal of communicating security information to end users.").

65. I note that in one of the @wangduoyu0 tutorial videos posted to Telegram, @wangduoyu0 highlighted a feature of the Lighthouse platform that automatically checks transparencyreport.google.com every 15 minutes to determine whether Google has flagged the phishing domain as malicious. That Google Transparency Report website includes the following information:

> Google's Safe Browsing technology examines billions of URLs per day looking for unsafe websites. Every day, we discover thousands of new unsafe sites, many of which are legitimate websites that have been compromised. When we detect unsafe sites, we show warnings on Google Search and in web browsers. You can search to see whether a website is currently dangerous to visit.[49]

The "Frontend Configuration" page of Lighthouse includes a toggle switch option labeled "automatically detect domain status." Moving this toggle switch to the "on" (green) position displays a message above the CMS phishing page template stating, "domain security detection rules (detected every 15 minutes), data from: transparencyreport.google.com." Below this message, the Lighthouse interface displays a legend for the indicator color that a user will see regarding the status of their phishing domain: green (normal), red (unsafe), orange (partially unsafe), or purple (no available data or test failed). Using a tool to monitor internet traffic on the computer running Lighthouse, I configured the Lighthouse CMS plugin and toggled the "automatically detect domain status" switch to the on position. Reviewing the resulting internet traffic, I observed that Lighthouse sent a "standard query" to "transparencyreport.google.com" and received a "standard query response" from "transparencyreport.google.com" including information from a Google domain name server. Approximately 15 minutes after the initial query and response, Lighthouse sent a "standard query" to "clientservices.googleapis.com" and received

[49] *See Safe Browsing Site Status*, Google Transparency Report (Jan. 29, 2025), https://tinyurl.com/456afbp4.

a "standard response" from "clientservices.googleapis.com." Following this response, Lighthouse received encrypted network traffic which indicates that Lighthouse is utilizing Google's technology and services to continuously monitor if a phishing site has been labeled as unsafe and is providing updates on the Lighthouse user interface.

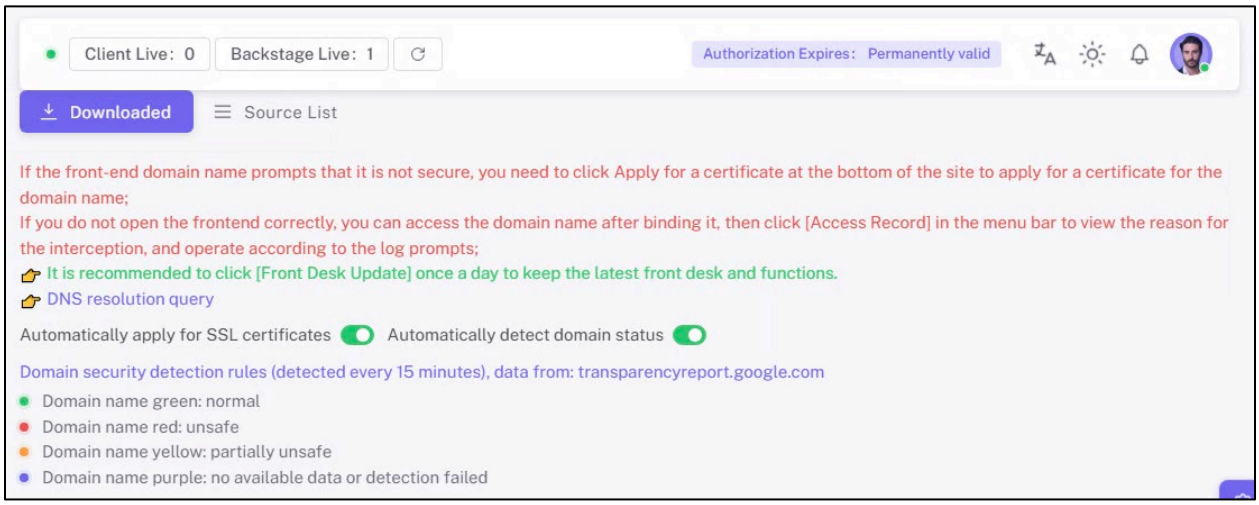


Figure 21. Screenshot of Lighthouse Software Displaying Domain Status Option and Color Legend

66. This step also allows a Lighthouse user to limit access to IP addresses from a certain country ("country whitelist") or to exclude those from a certain country ("country blacklist"). The use of IP address geolocation is a process used by Lighthouse phishing websites that acts as a gatekeeper to contain internet traffic to certain regions. The software also allows the user to divert potential phishing victims from a blacklisted country to a benign site of the user's choosing. In the configuration section for each domain, a URL can be entered in a text box labeled "blacklist address jump." The default site for the "blacklist address jump" in Lighthouse is https://google.com. This page also allows the user to set a default currency and payment price. Figure 22 depicts this "Frontend Configuration" step in the process.

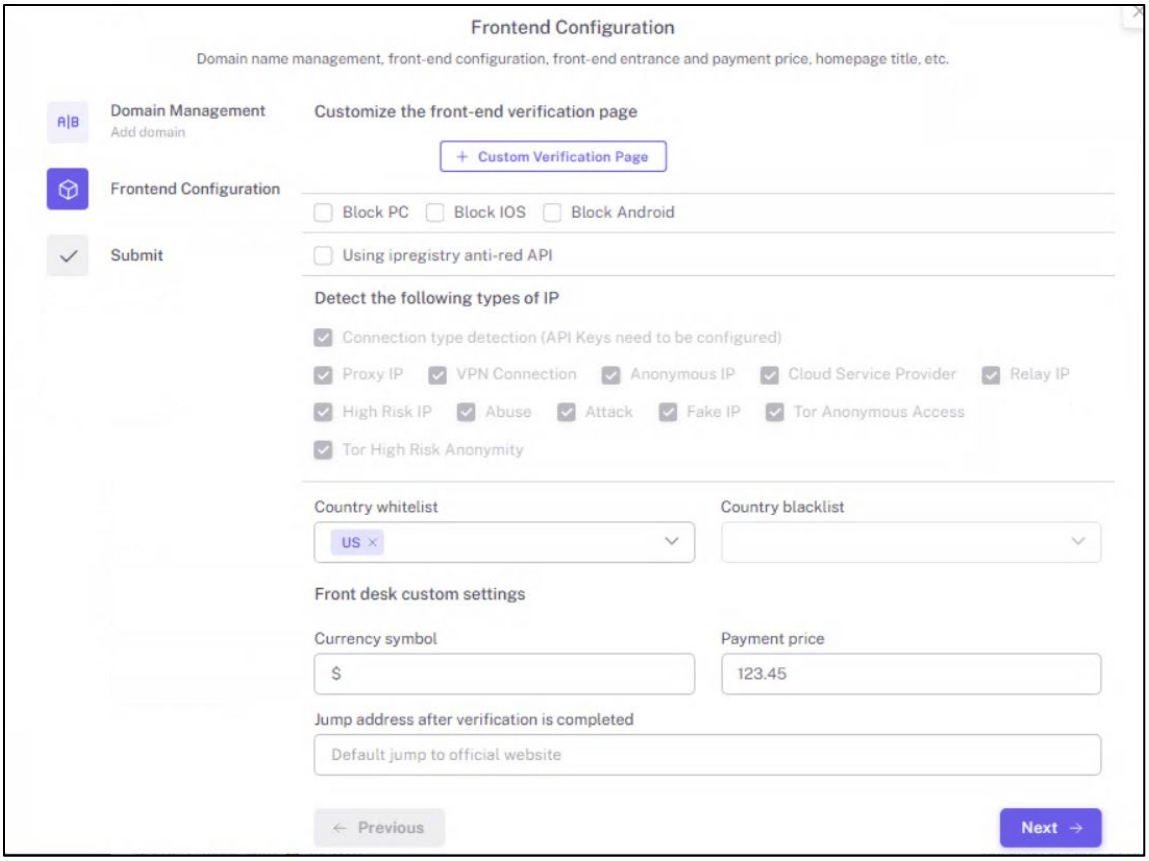


Figure 22. Lighthouse Frontend Configuration

67. Finally, the third step in the process, entitled "Submit," is a submission screen that displays the message, "Submit to kickstart your project," referring to the addition of phishing capabilities to the associated phishing website.

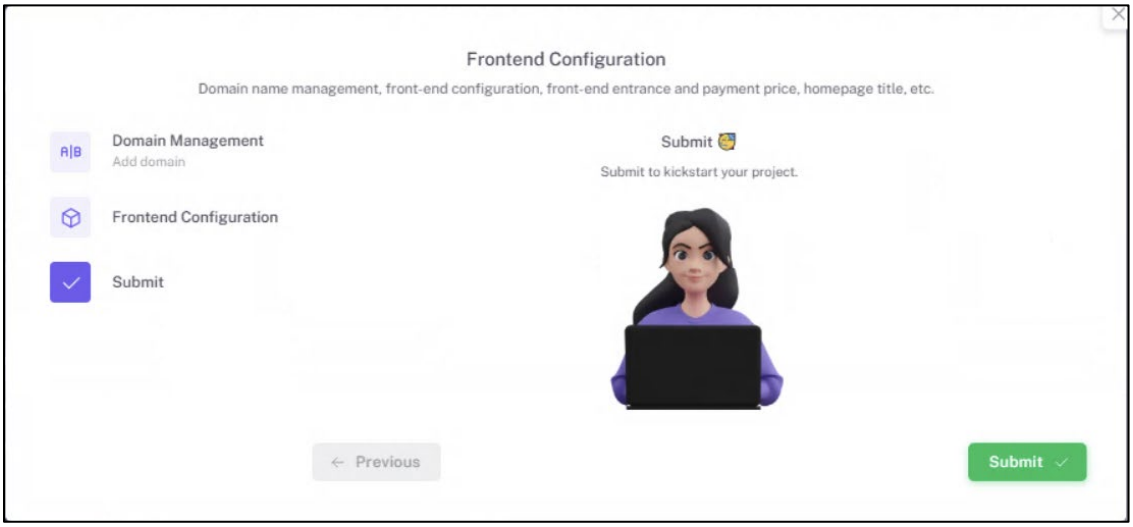


Figure 23. Lighthouse Frontend Configuration – Submit

68. Once a user has finished this process in Lighthouse, they connect the software to their fake e-commerce website (created using the CMS platform) by choosing the CMS platform's "add plugin" feature. Users are given the option to either install and activate plugins from a list of preloaded options or upload a custom plugin. Notably, one of the pre-loaded options is named "WooCommerce Stripe Gateway." This resembles the naming convention of the "Lighthouse Stripe Gateway" plugin that I downloaded from Lighthouse. In order to link a phishing website to Lighthouse, a user simply uploads the custom plugin Lighthouse Stripe Gateway to their website and configures it to connect with the phishing site, allowing the Lighthouse server to collect and store victim data.

69. Once a phishing website is activated, Lighthouse supports the collection of various types of data from victims. Of course, the ultimate goal of the phishing pages created with Lighthouse is to steal victim account information and subsequently take over the accounts. Some financial institutions implement MFA technologies to combat fraud, including sending numerical codes via SMS or through a dedicated mobile application, and certain features of Lighthouse enable the fraudsters to acquire these codes. On April 24, 2025, a Lighthouse tutorial video was posted on the Laowang Notice Telegram channel that displays this feature. Specifically, the video shows a Lighthouse user configuring the MFA functionality of Lighthouse to request that a phishing victim enter the code sent from their financial institution into a phishing page transmitted to Lighthouse.

70. According to the April 24, 2025, tutorial video, and my own familiarity with the software, I believe that Lighthouse subverts MFA protections in the following way. First, a victim navigates to a payment page on either a fake e-commerce or SMS phishing website. Once a victim

submits their payment information, which is funneled directly to Lighthouse, they are directed to a fictious MFA phishing page, prompting them to enter a code to verify their purchase.

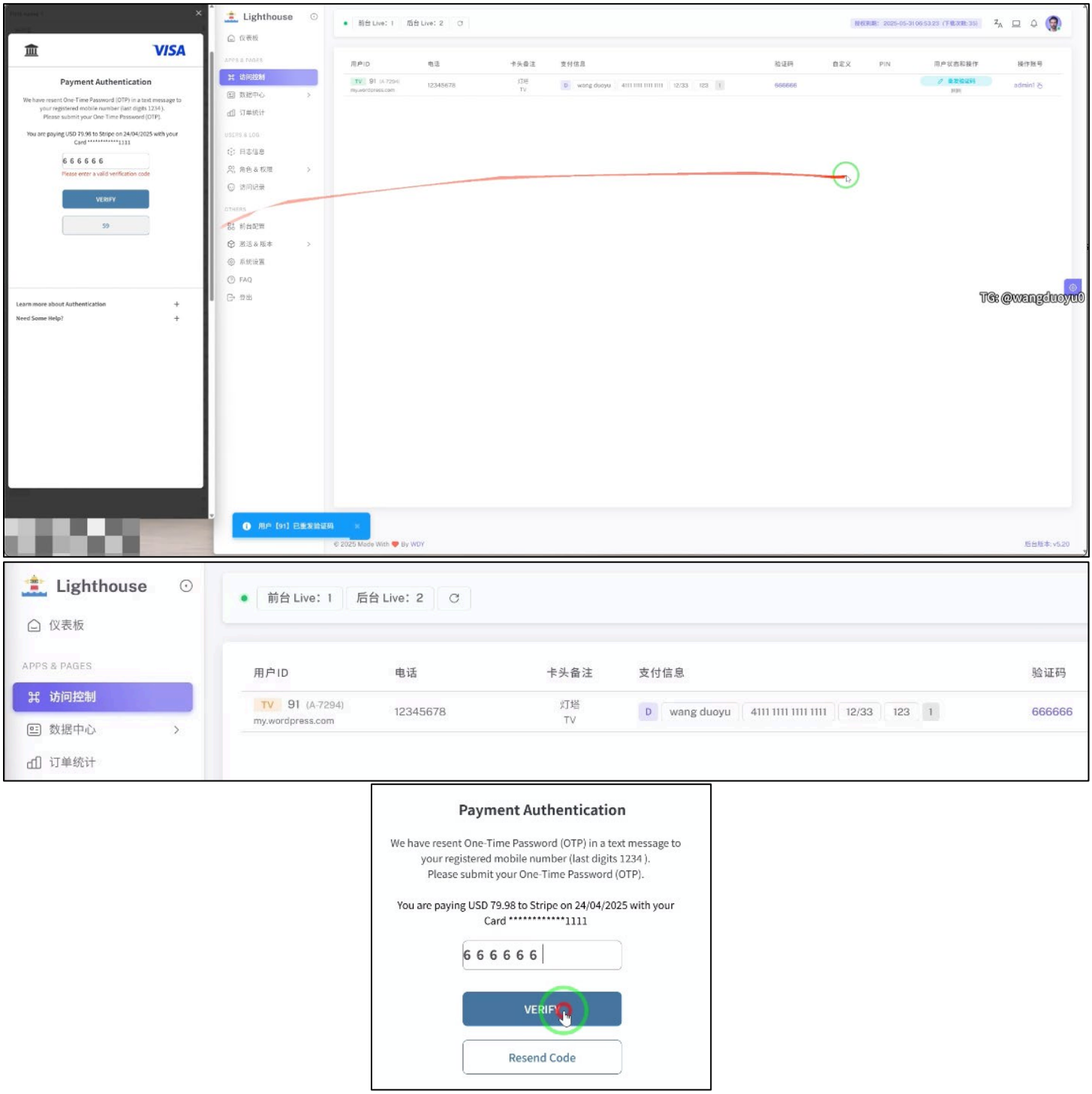


Figure 24. Screenshots from April 24, 2025, @wangduoyu0 Lighthouse Tutorial Video Displaying

MFA Functionality, https://t[.]me/laowang_notice/33 (translated)[50]

71. Lighthouse is configured to support various types of credit cards. For example, in the tutorial, Lighthouse recognized that the victim entered a Visa card number and sent them an MFA page with the Visa logo, requesting a code with the number of digits that a typical Visa MFA code would contain. While the victim waits to receive the code, the scammer uses Lighthouse to generate a visual representation of the victim's credit card.

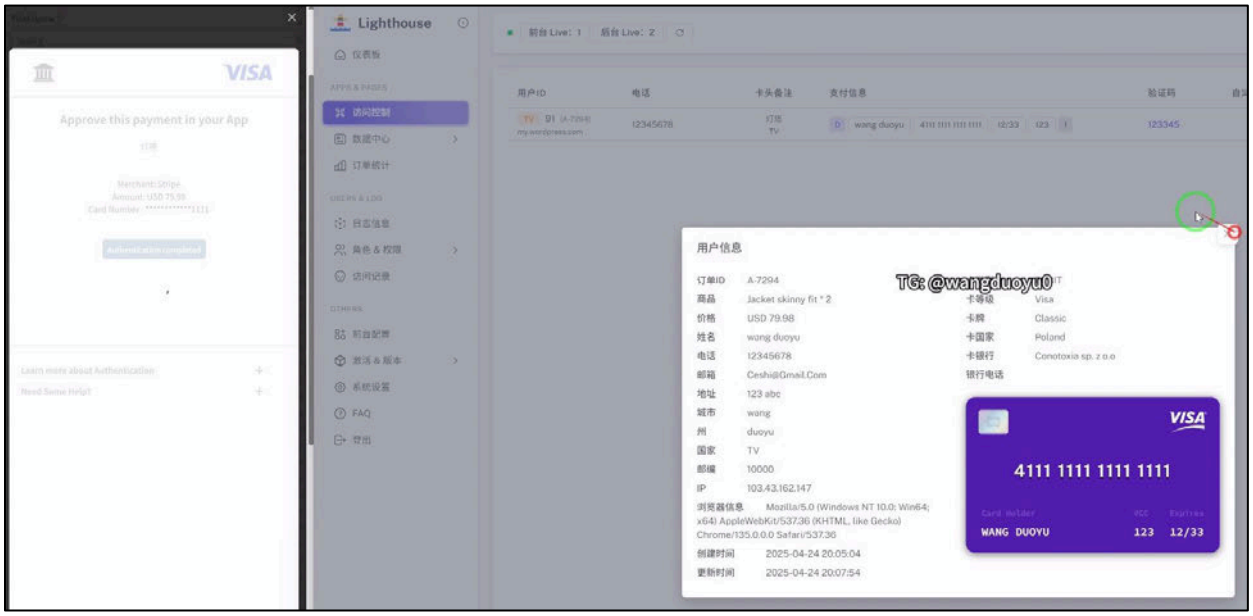


Figure 25. Screenshot from April 24, 2025, @wangduoyu0 Lighthouse Tutorial Video Displaying Ability to Generate Visual Representation of Victim Credit Card, https://t[.]me/laowang_notice/33 (translated)[51]

72. The scammer then scans this Lighthouse-generated card image with a camera on a mobile device and attempts to add the payment method to a wallet application (like Google Wallet) on the mobile device. Attempting to add the credit card as a payment method on a mobile device triggers the card's financial institution to send an actual MFA code to the victim. The victim, believing that the code is being received in response to the purchase authorization, (and not

[50] Ex. 1 at 35–37.
[51] Ex. 1 at 41.

realizing that it is in fact authorizing the fraudster to add a payment method to a mobile device) enters the code into the MFA phishing page.[52] The scammer receives the code through Lighthouse and inputs it on their mobile device, using it to authorize adding the payment method to their mobile device's wallet. Once the victim's payment method is added to the mobile device, it can be used for fraudulent transactions without the need for additional MFA codes.

73. A similar process, demonstrated in an April 24, 2025, video posted to the Laowang Notice Telegram channel, is used to trick phishing victims into entering account information from payment platforms like PayPal. In this tutorial video, the phishing victim appears to click on the button labeled "Click the PayPal button below to process your order" and is directed to a webpage with the title "Pay with PayPal" with text boxes that read "Email or mobile number" and "Password." The phishing victim enters an email address and password, both of which immediately appear in the Lighthouse software. The scammer selects from a list of options in the software, one of which reads "Release; verification card number" and another which reads "Release; PP Google Verification."[53]

[52] I know that many mobile phones automatically capture MFA codes from text messages, allowing people to directly input them into a webpage without navigating to the text message. Therefore, even if the text message with the MFA code would otherwise alert a user that their card was being added to a wallet, victims who use the one-click option to enter the code would never read the message.

[53] Although not pictured in the tutorial video, I believe that if the threat actor selected "Release; PP Google Verification," the potential phishing victim would be presented with a phishing page to enter a code from their Google Authenticator application.

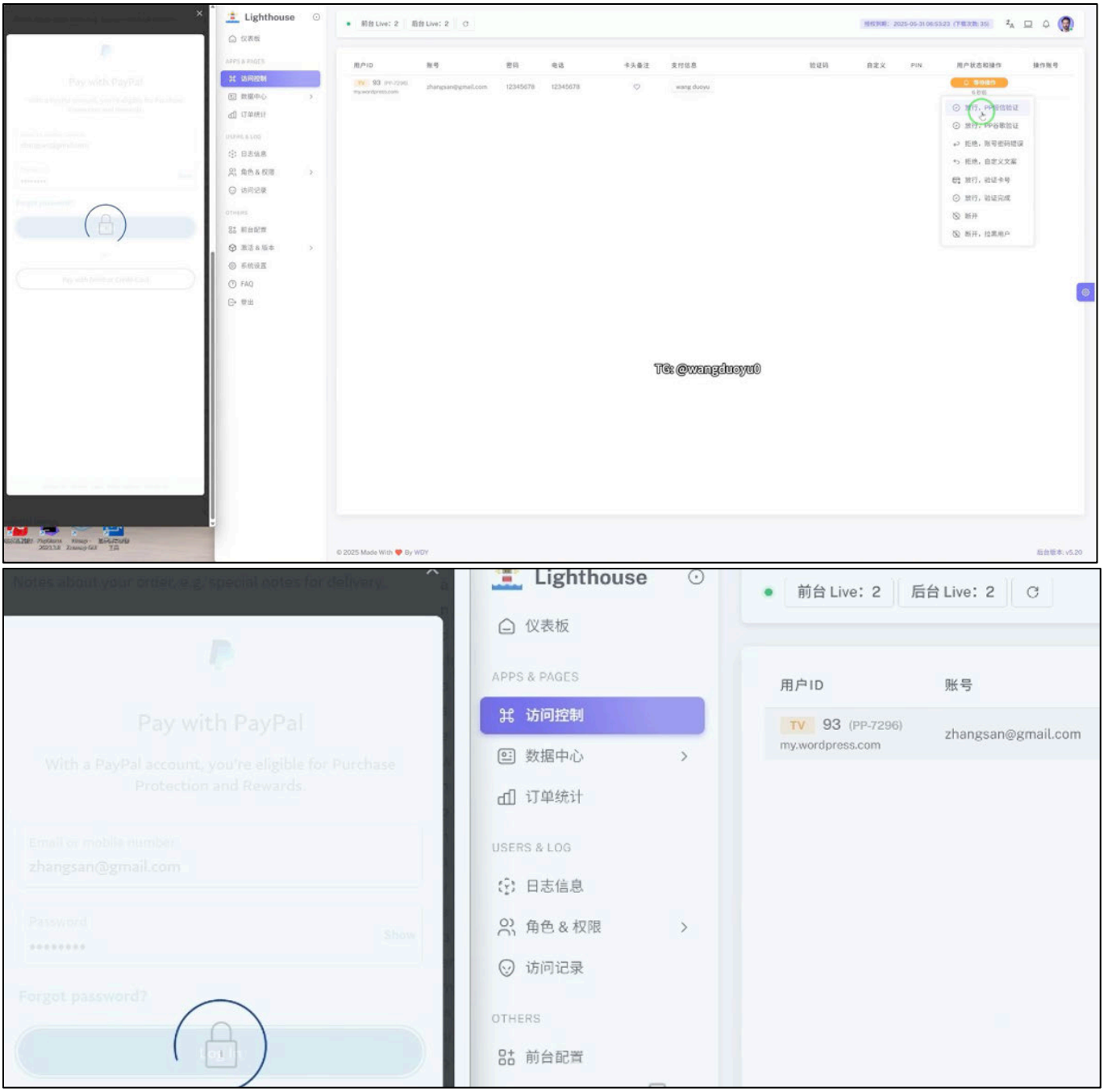


Figure 26. Screenshots from April 24, 2025, @wangduoyu0 Lighthouse Tutorial Video Displaying Victim View While Scammer Manipulates Software (translated)[54]

74. In this context, I understand the term "PP" to refer to PayPal. In the tutorial, the Lighthouse user selects the SMS verification option which brings up a pop-up window that reads

[54] Ex. 1 at 49–51.

"SMS verification guide. Please enter the mobile phone number format." The Lighthouse user enters the victim's phone number. As the scammer is working in the background, the phishing victim is viewing the "Pay with PayPal" page with a lock and a spinning circle, indicating that information is still loading. After the scammer clicks "submit" in the pop-up window, the potential phishing victim is presented with a webpage with the PayPal logo with a message that reads "Let's confirm it's you" with a radio button stating, "Get a text" followed by "Mobile" and the victim's phone number. The potential phishing victim clicks the "next" button and is presented with a page with the PayPal logo followed by "Enter your code" and "We've sent a security code to," followed by their phone number.

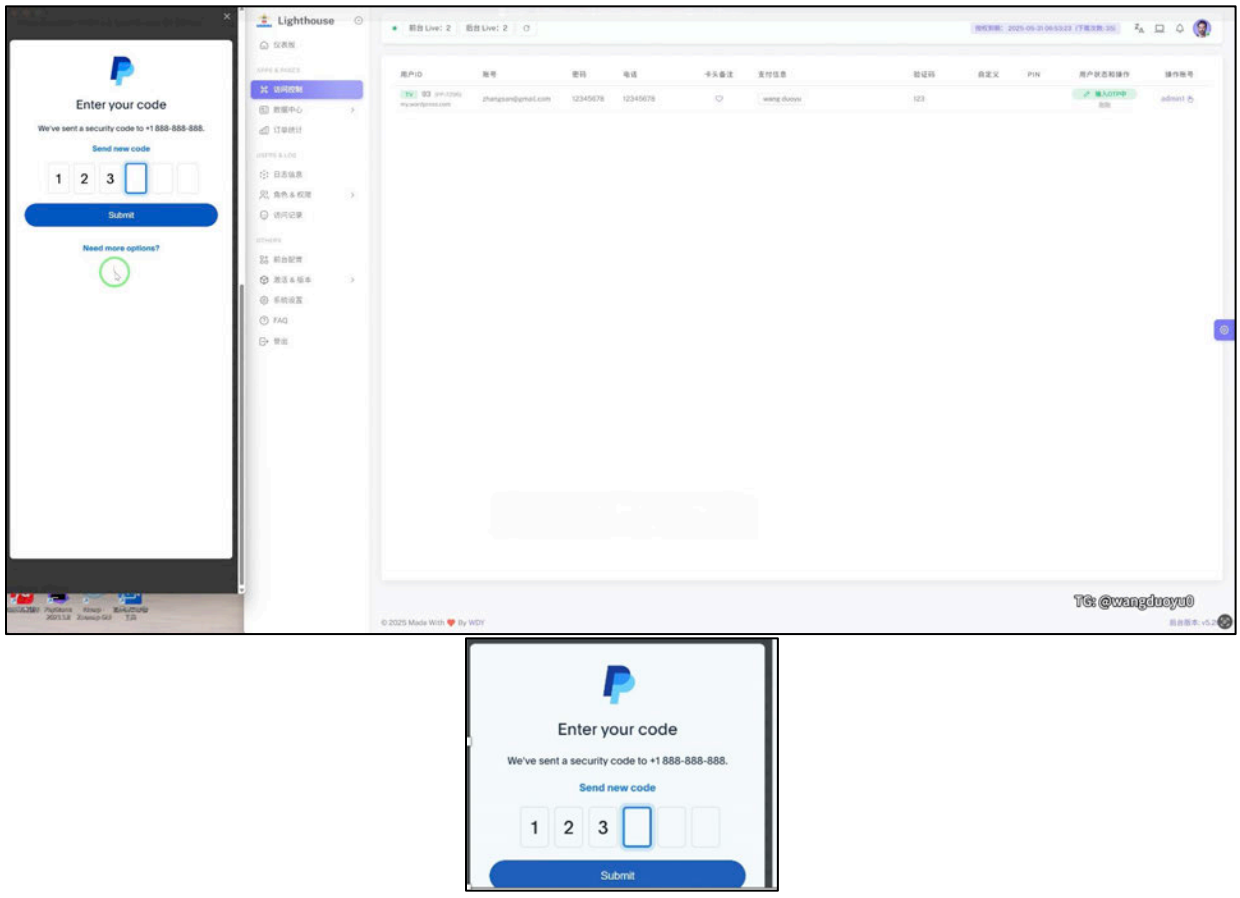


Figure 27. Screenshots from April 24, 2025, @wangduoyu0 Lighthouse Tutorial Video – Victim Entering MFA Code (translated)[55]

[55] Ex. 1 at 55–56.

75. Although not visible in the video, I believe that at this point in the scam, the fraudster attempts to log in to the victim's PayPal account, prompting an MFA code to be sent to the victim's phone. The phishing victim receives a verification code from PayPal which they enter into the phishing website, allowing the fraudster to successfully access the victim's PayPal account.

76. Even after having accessed the PayPal account, Lighthouse allows the scammer to choose an option that reads "Release, card verification." The phishing victim is then presented with a webpage with a message at the top in a yellow background, that reads "As part of an update to the payment system, confirmation of your registered credit card is required to verify your identity. Other payment methods are currently unavailable." The potential phishing victim is then prompted to enter a credit card, potentially allowing the fraudster to steal two payment methods.

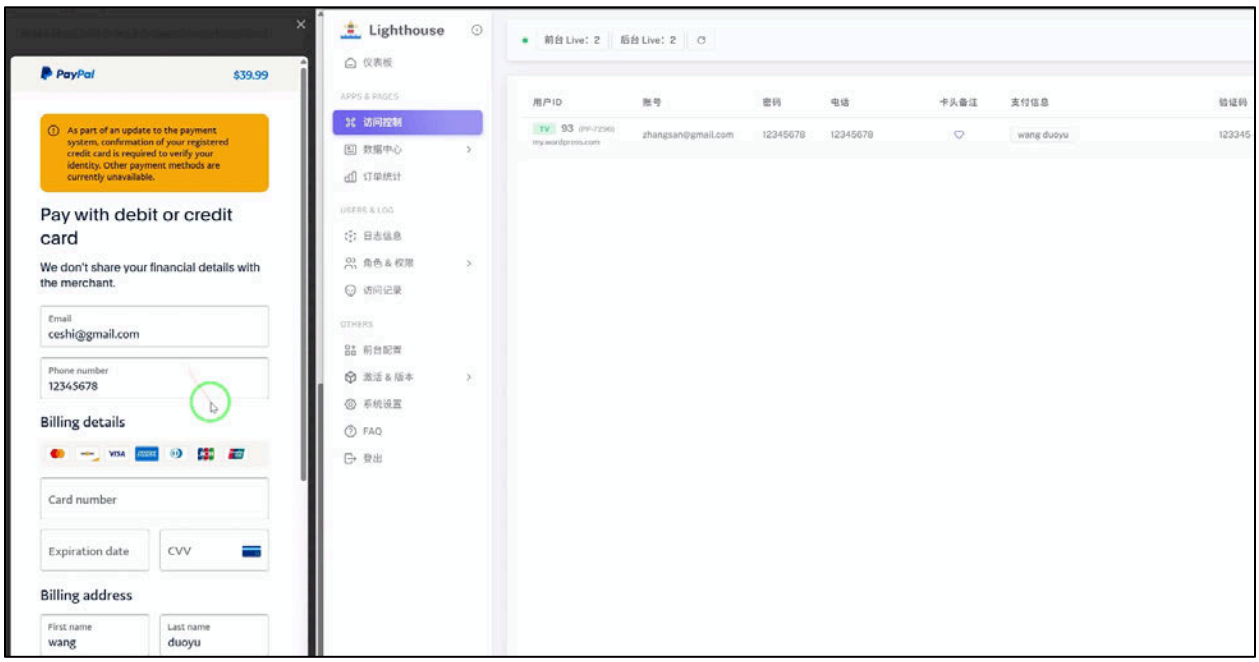


Figure 28. Screenshot from April 24, 2025, @wangduoyu0 Lighthouse Tutorial Video Displaying Secondary Payment Information Attempt (translated)[56]

[56] Ex. 1 at 60.

77. The use of these features of Lighthouse requires the fraudster to be sitting at their computer while the victim is accessing the fraudulent website in order to prompt the software to display the appropriate webpages, and to log into victims' accounts in real time.

78. I also note that Lighthouse does not require a victim to affirmatively send information by clicking, for example, a "submit" button, but instead collects victim-inputted data in real time as they type. I confirmed this by visiting a phishing page I identified as being created with Lighthouse (using the fingerprinting techniques outlined below) with the URL [redacted].

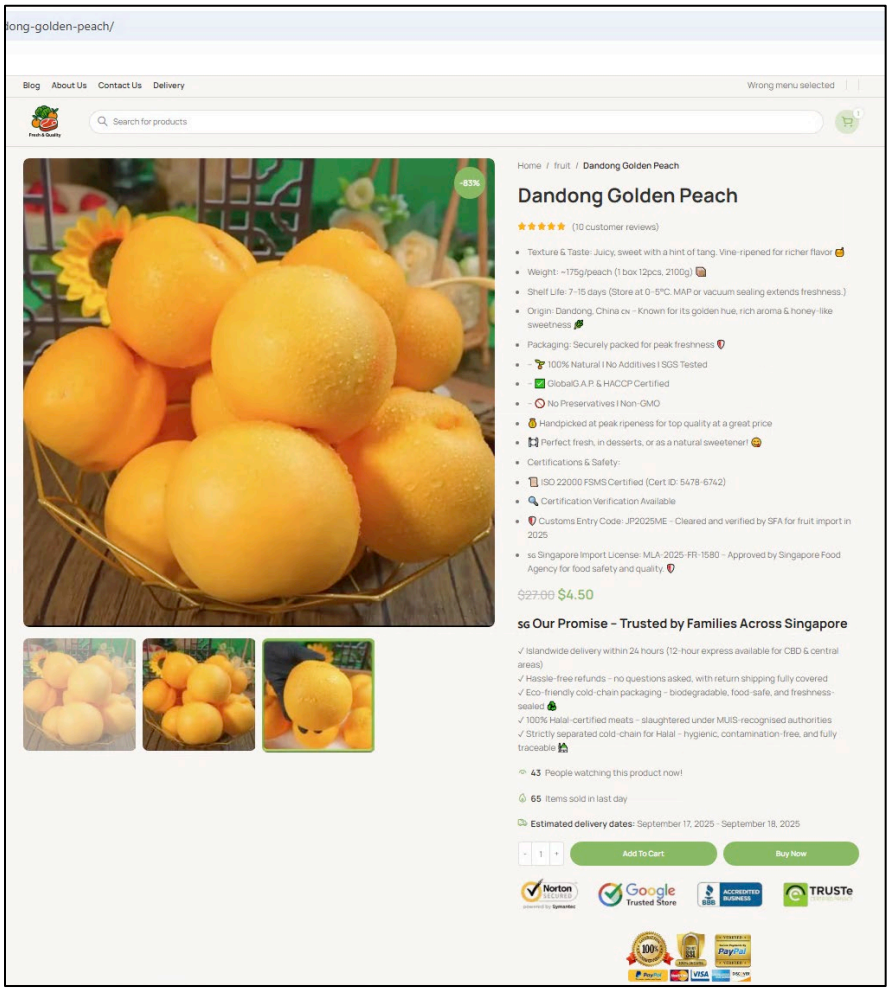


Figure 29. Screenshot of Lighthouse-Created Phishing Website Visited September 16, 2025[57]

[57] I note that the page displays the Google logo along with the words "Google Trusted Store," apparently to give credibility to the fake website.

79. I added a product to my shopping cart and began the checkout process. The first text entry box was labeled "email address." I entered some test information and monitored the network activity between my browser and the phishing site using the developer tools option in the Google Chrome browser, which allows for the inspection of website resources and other information that occurs behind the scenes when a user visits a website. Specifically, in the email box I typed, "I am not pressing submit." A connection named "ws" appeared at the top of the list of files supporting the functionality of the website. In this context, I know that "ws" refers to WebSocket, a communication protocol that provides real-time, persistent connections between a client, such as a web browser, and a server. A review of the data sent between my web browser and the Lighthouse phishing page, shows a continuous stream of "ping" and "pong" messages sent and received using the WebSocket connection. The ping/pong mechanism is used by WebSocket connections to maintain a persistent connection between the client and a server. A review of the XHR file named "?wc-ajax=update_order_review" underneath the WebSocket connection displays the "payload" (data sent from the web browser to the Lighthouse software) and lists the payment method as "woocommerce_payments_lighthouse_gateway." It also listed a billing email as "I am not pressing submit," which matches what I entered into the email field on the phishing page.

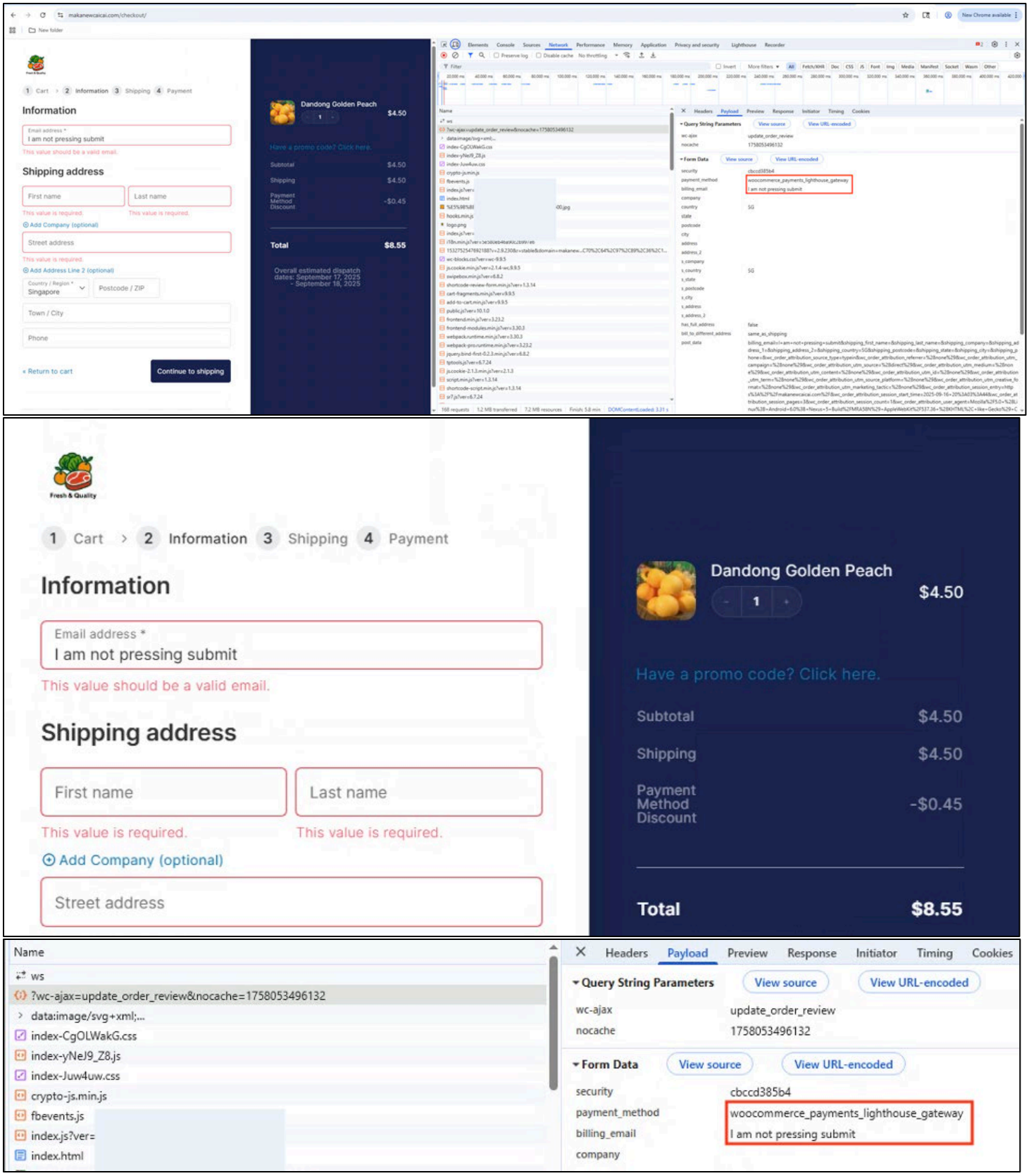


Figure 30. Lighthouse Phishing Page Illustrating WebSocket Functionality

80. I believe that users of Lighthouse use this WebSocket connection process to collect live data from potential phishing customers, without the need for them to hit a "submit" button. The result is that potential victims who begin to enter data on the phishing page, and then discover that they are being scammed, can still have data stolen even if they do not complete the order process.

81. The WebSocket connection initiated on the phishing website to steal victim data is also a way to identify the Lighthouse software servers, those used by phishing scammers to host Lighthouse and collect victim data. As the user inputs information into the phishing site, the WebSocket connection transmits data directly to the Lighthouse server(s) that is under the command and control of the threat actor(s) overseeing the phishing campaigns. Using the WebSocket identification process outlined above, I visited phishing websites created with Lighthouse (the identification method for which is described *infra*) and monitored the network connections made between the sites and their respective data collection servers. Using the developer tools option within the Google Chrome browser, I selected the WebSocket connection and observed the "Request URL" that was sending and receiving data between the phishing site and the Lighthouse server.

82. For example, I identified the URL [redacted] as a Lighthouse-created phishing website. I entered data into the fields on the checkout page and noticed that the WebSocket connection transmitted data to the requesting URL, wss[:]//verify.securitytops[.]com/ws,[58] indicating that it was the server receiving victim data from the phishing website. A query for information related to the securitytops[.]com domain reveals

[58] The domains in this declaration that are not redacted are not on Appendix A because they did not meet the criteria for inclusion.

that it was registered on August 21, 2025, using the registrar Dominet Limited via Alibaba Cloud. According to DomainTools, a service that provides information on domains, IP addresses, and service providers, the securitytops[.]com domain is labeled with a "phishing" threat label, warning that it has been associated with phishing website activities.

83. I repeated this process using multiple Lighthouse phishing pages and identified the WebSocket connections with their respective data collection servers. Some phishing sites with different hostnames and URLs shared the same data collection server, meaning they were operated by the same phishing operation. Additionally, some phishing sites had connections to different Lighthouse software servers on different days.

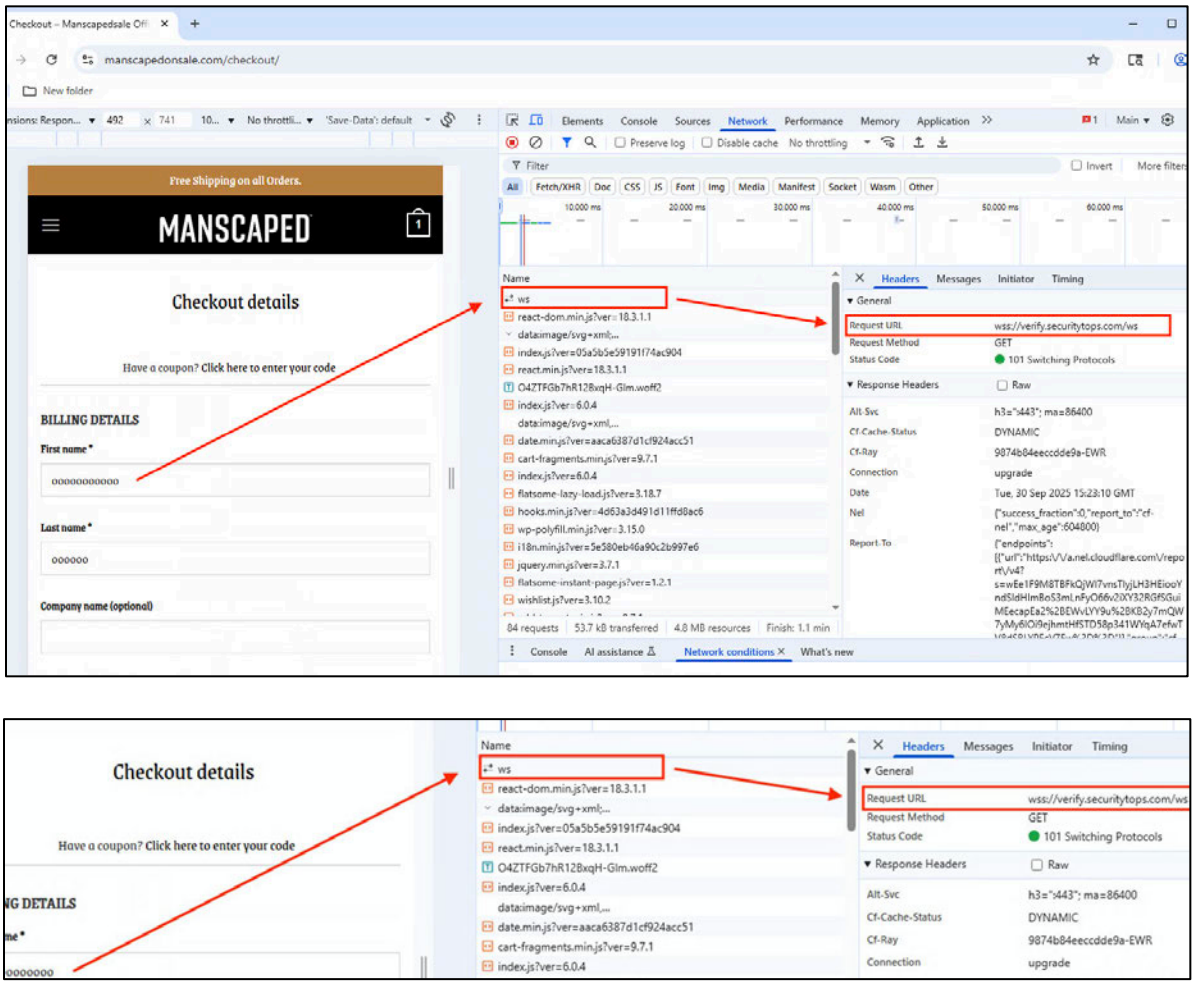


Figure 31. Lighthouse Phishing Page Illustrating WebSocket Connection to a Data Collection Server

IV. Identifying Lighthouse Phishing Domains

84. To identify active domains hosting phishing websites created with Lighthouse, I used my analysis of the software to pinpoint unique "fingerprints" of the Lighthouse sites. As will be discussed in more detail herein, I identified one file that I believe is unique to e-commerce sites created with the CMS platform and another file that I believe is unique to SMS sites created with certain Lighthouse templates. I then searched active domains that contained these specific files. In total, I identified approximately 2,600 domains from 2024 to the present that remain active. The domains and a list of registrars hosting those domain names are attached as **Appendix A**. Even though some of the websites do not currently display content, as long as the domains remain active, they could easily come back online.

85. I note that my searches will return only a subset of Lighthouse-created websites for a number of reasons. They will not likely locate phishing websites made with the Chinese e-commerce platform, custom SMS websites, or SMS websites using certain templates that did not include the specific file I identified. Additionally, I searched for websites with the fingerprints I identified using URLScan.io, a repository of publicly submitted websites that have been scanned and preserved. When a website is submitted to URLScan.io, URLScan.io automatically browses to it and records activity including "the domains and IPs contacted, the resources (JavaScript, CSS, etc.) requested from those domains, … cookies created by the page" and more. It will also take a screenshot of the page.[59] Websites that were not affirmatively submitted by internet users to URLScan.io would therefore not be identified in my search. Additionally, many of the websites I did identify displayed the Lighthouse fingerprint on subdomains, a prefix added to a main domain

[59] *See About*, URLScan.io (last visited Nov. 6, 2025), https://tinyurl.com/44zh8ypp.

name. For example, in "example.google.com," example is the subdomain, and Google is the apex domain. Appendix A includes only those websites in which the Lighthouse fingerprint was found on the apex domain, or those in which the apex domain either automatically redirected to the subdomain containing the fingerprint or had only one subdomain, which contained the fingerprint. Although I think it is quite likely that each apex domain I identified is utilized only to host phishing websites, I limited the domains included on Appendix A in this way out of an abundance of caution.

86. As discussed previously herein, I believe that the "Lighthouse Stripe Gateway" plugin is unique to websites funneling data to Lighthouse, and therefore can be used as a way to identify e-commerce phishing websites created with Lighthouse. I used this "fingerprint" to search for active domains employing the plugin. On August 18, 2025, my search revealed over 1,000 potential phishing websites using this plugin. I reviewed over 100 of these and determined that all of them appeared to be consistent with fraudulent e-commerce websites created on the CMS version using the Lighthouse plugin. I also directed and supervised a team at NAXO that confirmed that all of them appeared to be consistent with fraudulent e-commerce websites created on the CMS version using the plugin.

87. For example, on August 18, 2025, I visited WoadMist DOT shop, an apparent e-commerce site offering various food items for sale. The website displays a storefront with categories of different goods along with a heading that claims, "Safe Payments. Secure payment, Don't keep any cards information [*sic*]." Figure 32 depicts the home page of the website.

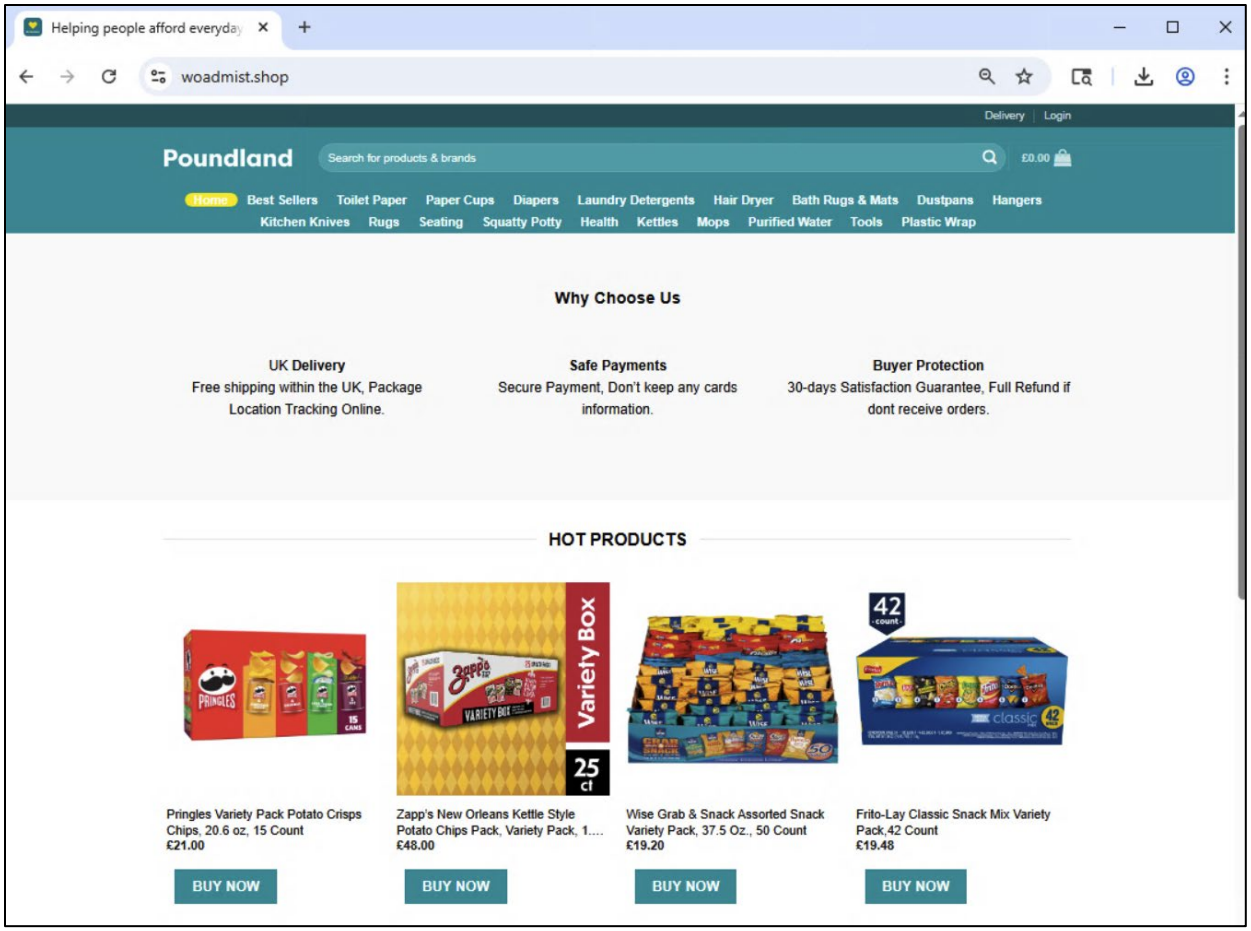


Figure 32. Suspected Phishing Website Using Lighthouse Gateway Plugin

88. After choosing an item to "purchase" I navigated to the checkout page which asked for shipping and payment information. Utilizing the Google Chrome browser, I enabled developer tools. I observed a folder named "wp-content" which is commonly used by CMS websites to store files and information. Inside of the "wp-content" folder was a "plugins" folder containing nine additional folders. One of these folders was named "lighthouse-stripe-gateway/assets" which contained files that appeared consistent with those contained in a CMS plugin. Using hash values, I confirmed that these files exactly matched files provided with Lighthouse. Figure 33 depicts the checkout page and Chrome developer tools view.[60]

[60] If a victim were to input their payment information, the website would direct them to a landing page that would indicate that the purchase had been completed, likely including a tracking or other

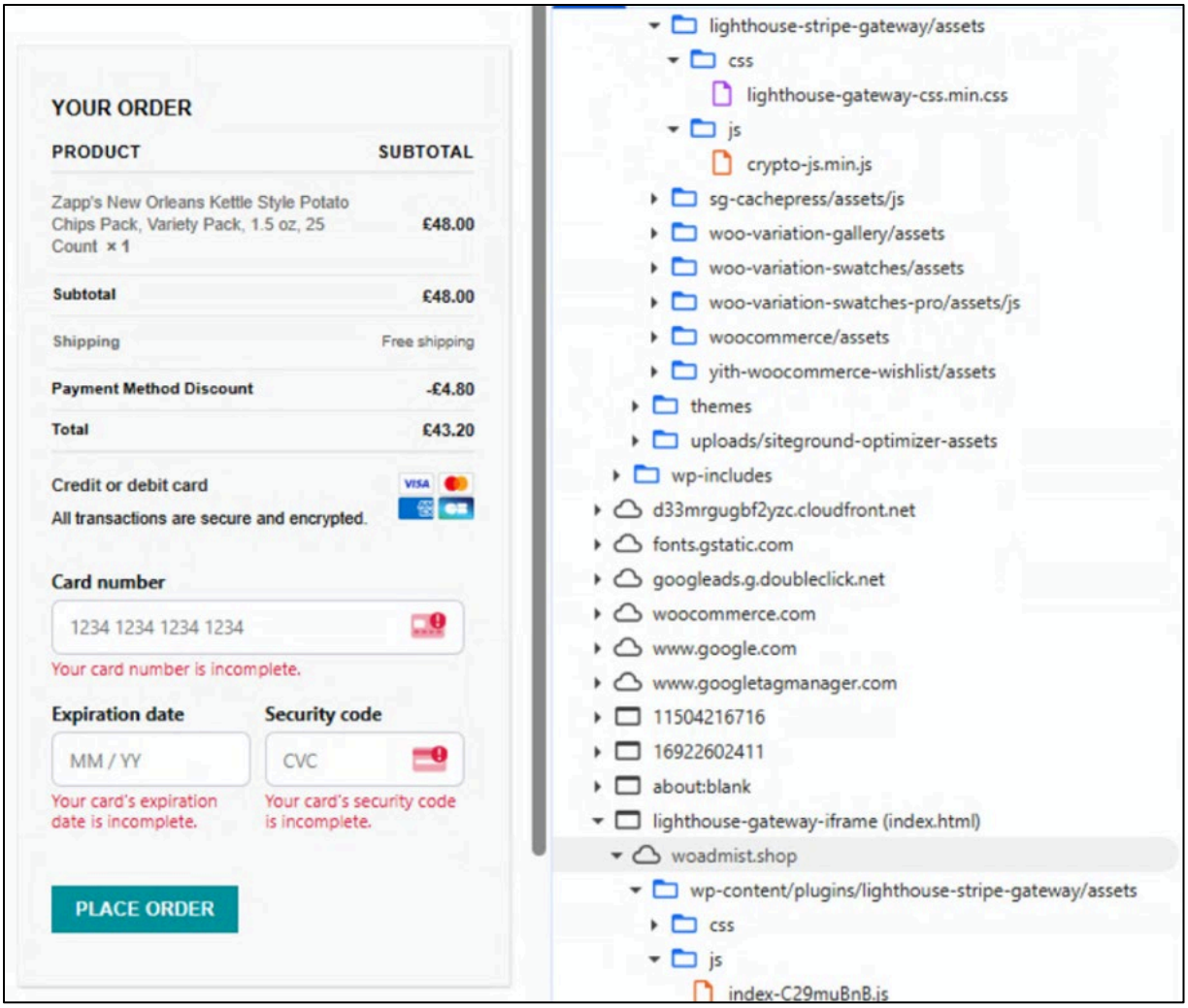


Figure 33. Checkout Page and Evidence of CMS Lighthouse Plugin

89. Although the version of the software I activated only allowed the creation of e-commerce phishing websites, activation of the software nevertheless allowed me to download and review the SMS phishing template files. I opened and reviewed the USPS phishing template. Extracting a file labeled "usps.zip" revealed a folder named "assets" and three files, "favicon.ico," "index.html," and "robots.txt." Opening the "favicon.ico" file displayed the USPS eagle head logo. The "assets" folder contained 33 files, many of which are images of logos of known financial

confirmation number. In reality, the victim would never receive their purchase and the Lighthouse user would simply have stolen their information.

institutions and credit card issuers. One of the 33 files in the assets folder is named "loading-WdnO4B_X.jpg" which is an animated image file of a spinning wheel of hashmarks. This animation is commonly used when information is in the process of being loaded to a webpage.

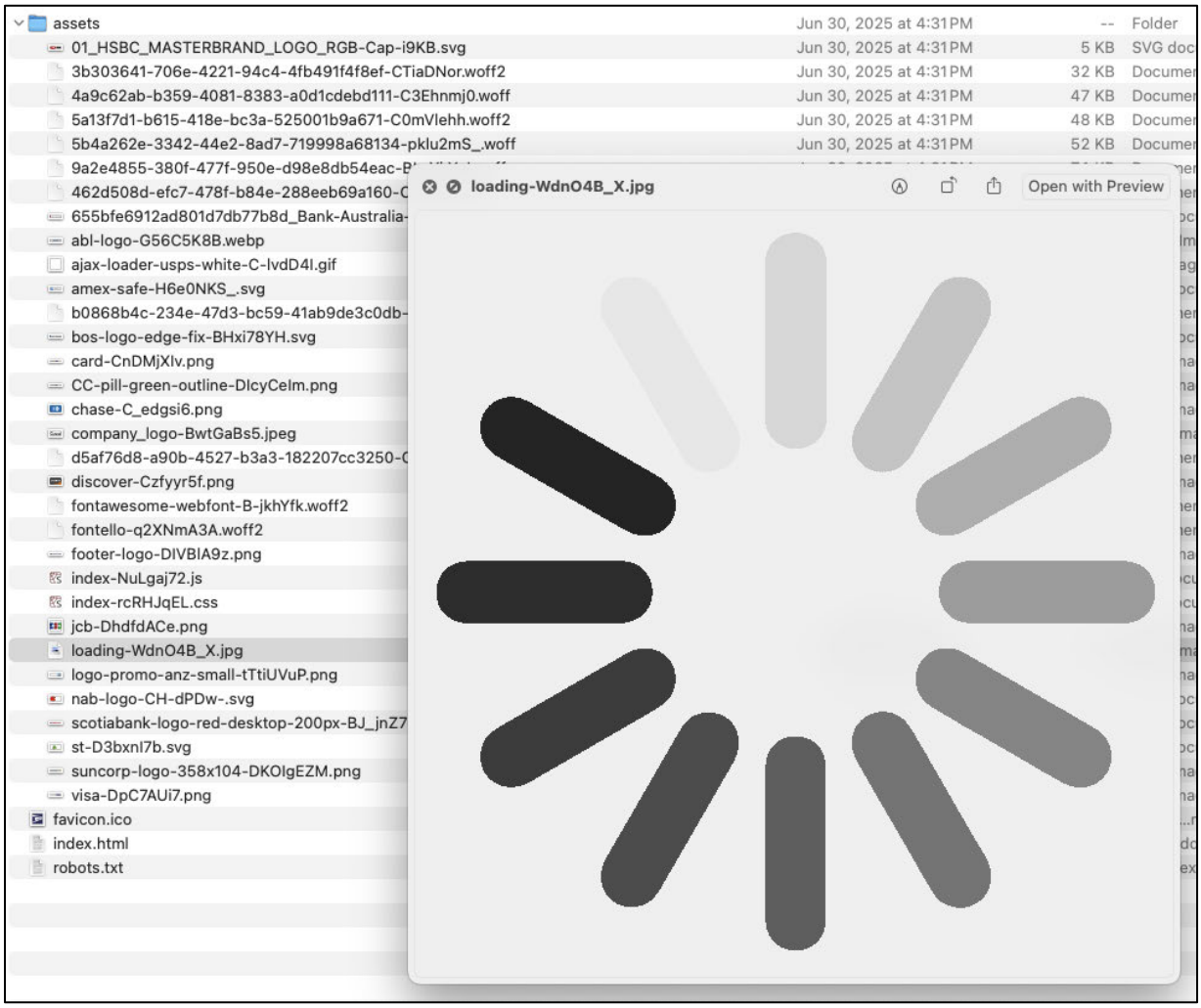


Figure 34. loading-WdnO4B_X.jpg from the Lighthouse USPS Template

90. Using the "loading-WdnO4B_X.jpg" image file as a possible fingerprint to identify active phishing sites, I searched for domains that utilized this file in the configuration of webpages. On August 19, 2025, the first and most recent search result was the domain, "http://fidelity-click[.]top/us." When I visited the webpage on my Google Chrome browser, I received an error stating, "[t]his site can't be reached." Utilizing the option within developer tools to emulate a browser on a mobile device, I was able to reload the webpage, revealing a red screen because the

browser had flagged it as dangerous. After continuing through the warnings, the webpage displayed a financial institution login screen with text boxes to enter a username and password. I observed that the page utilized the "loading-WdnO4B_X.jpg" image file which was stored within a folder named "assets." Comparing the "loading-WdnO4B_X.jpg" file downloaded from the phishing page with the "loading-WdnO4B_X.jpg" file extracted from the Lighthouse platform template using the MD5 and SHA1 hash algorithms confirmed that the files are identical.

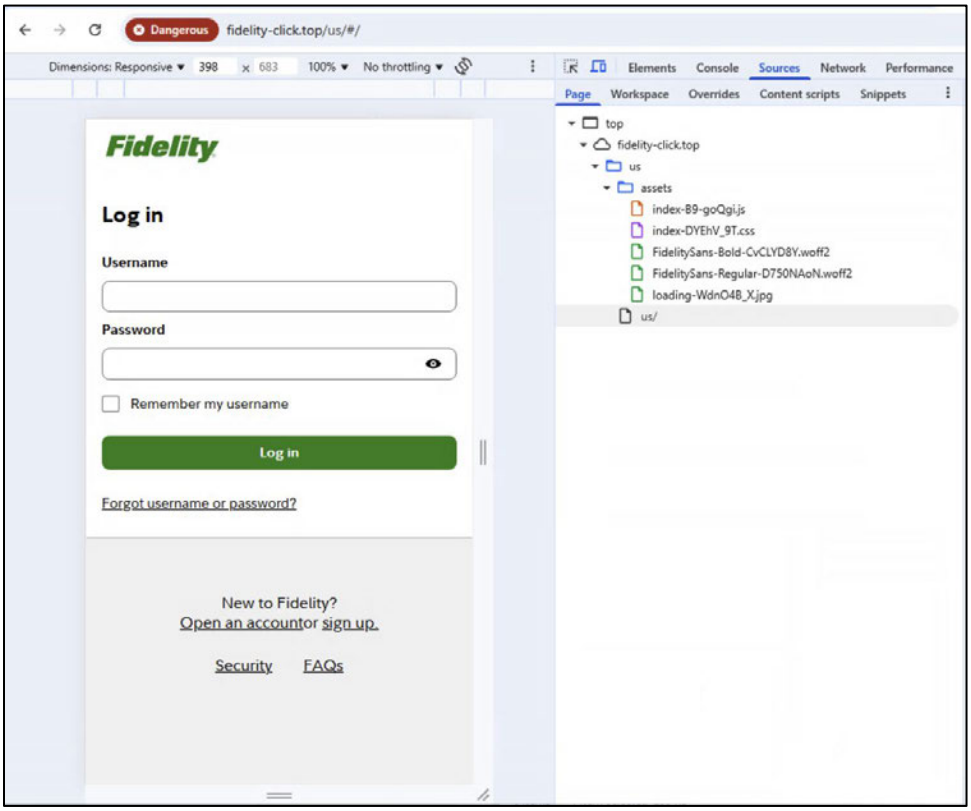


Figure 35. Phishing Website Identified Using the loading-WdnO4B_X.jpg File

91. Using this search, I manually reviewed a randomly selected sample of over 100 hostnames and every one of them had clear indicators of a phishing website. Another website found during my search showed the New York E-ZPass scam template in use at the website "rhyss[.]win." The screenshot below was captured on February 19, 2025. I confirmed that the website contained the file "loading-WdnO4B_X.jpg" and the image "logo_ezpass-2-

Dmuz3_ks.gif." Both files appear in the "ezpassny_us_etc" Lighthouse template and both files' SHA-225 hashes match the hashes of the website's images.

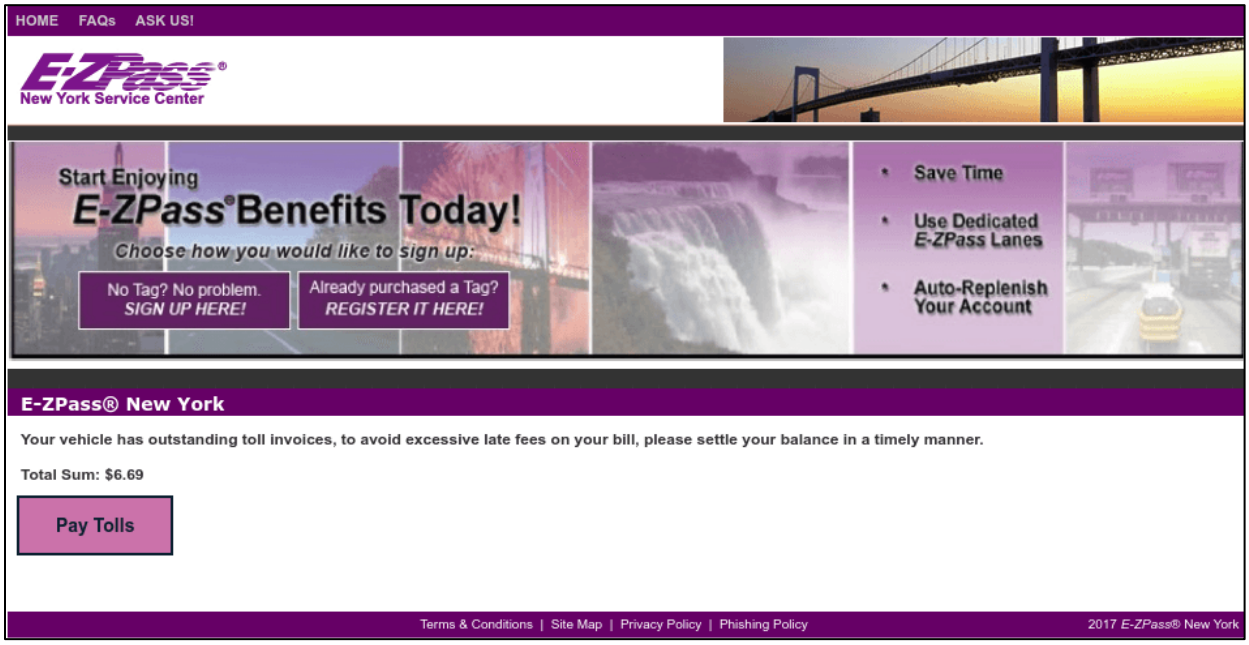


Figure 36: Screenshot of E-ZPass New York Phishing Website Captured Using Search Criteria February 19, 2025

92. On or about November 4, 2025, I ran new searches using each of the two methods discussed herein. I found approximately 2,591 unique domain created from August 24, 2024, through November 4, 2025.

V. Telegram Users and Sale of the Lighthouse Software

93. Telegram user @wangduoyu0 claims to have developed Lighthouse and offers it for sale through several Telegram channels. Those channels are referenced on @wangduoyu0's Telegram profile.

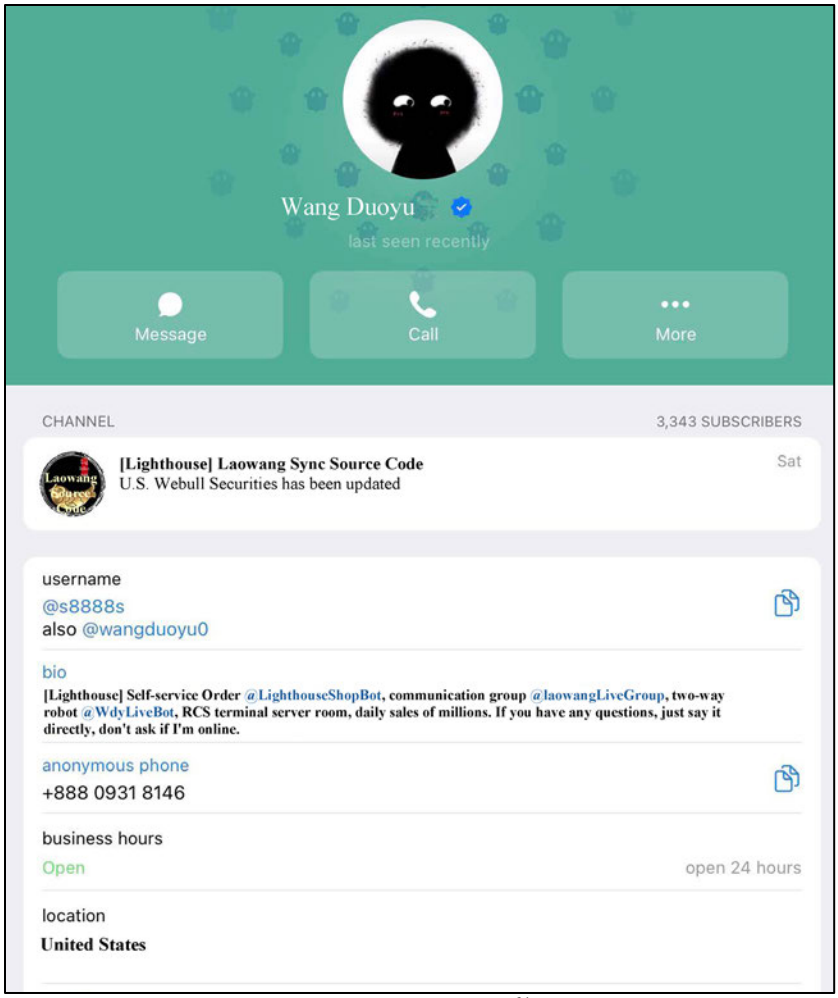


Figure 37. @wangduoyu0 Telegram Profile (translated)[61]

94. I reviewed all the channels and groups linked to @wangduoyu0. The @laowang_notice channel is used almost exclusively to post advertisements for updates to Lighthouse and tutorials for how to use the software. For example, on May 17, 2025, the channel posted an announcement that it would host a new "self-service order bot."

[61] Ex. 1 at 64.

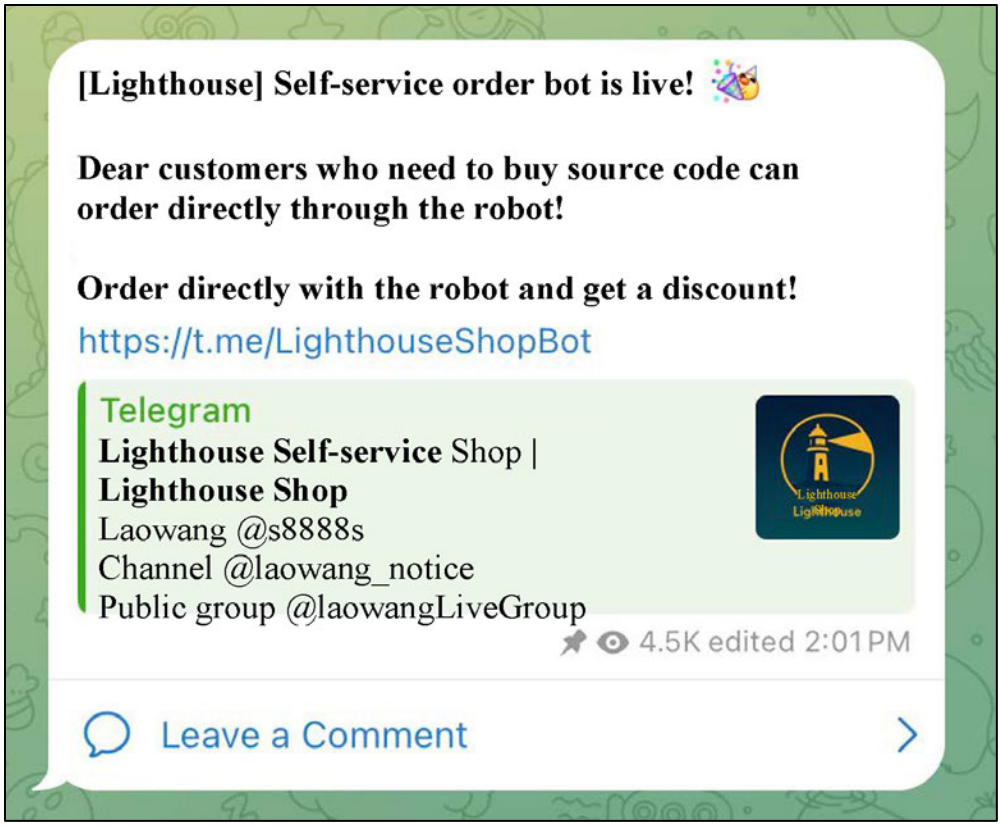


Figure 38. @wangduoyu0 Post in @laowang_notice Channel, https://t[.]me/laowang_notice/67 (translated)[62]

95. The @laowangLiveGroup, described in @wangduoyu0's profile as a "communication group," is a Lighthouse-related discussion group with over 2,500 members. It is run by a group of seven Telegram users (including @wangduoyu0) who all appear to provide services to support the Lighthouse phishing operation. In this group, Telegram users post openly about engaging in fraud. For example, on July 31, 2025, at 3:11 p.m., one user posted, "Who can send a few US live baits?" followed by two laughing emojis. At 3:42 p.m., another user asked, "Who is fishing? Looking for a partner." At 4:15 p.m. and 4:59 p.m., two other users posted "online."

[62] Ex. 1 at 68.

Figure 39. Posts in @laowangLiveGroup, https://t[.]me/laowangLiveGroup/18430, 18449, 18459, 1846267[63]

96. On August 2, 2025, at 5:20 a.m., a user posted, "selling pure handmade wealthy accounts with Zel activation, telegraphic transfer accounts, Apple CASH ID, those who understand, come." I believe that this user was attempting to sell account information that he or she had successfully phished. They advertised that the accounts were "wealthy" and had Zelle activation which I know to be a digital payment network that allows transfers between financial institutions.

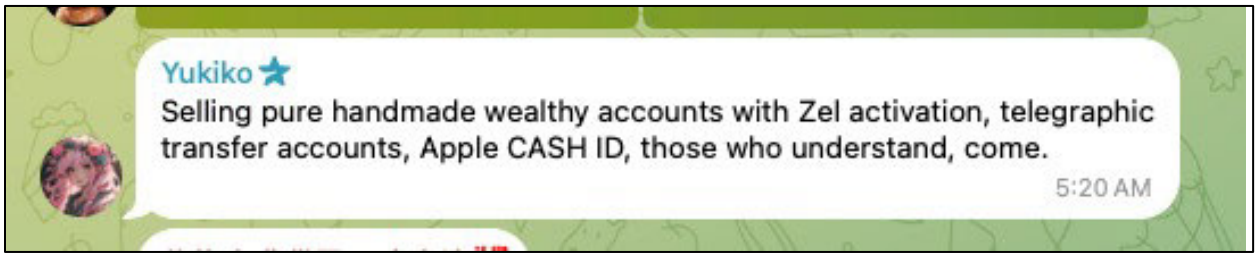


Figure 40. Post in @laowangLiveGroup, https://t[.]me/laowangLiveGroup/19255[64]

[63] This screenshot includes text translated by Telegram's translation function. Exhibit 1 includes the original message and a certified translation. *See* Ex. 1 at 72.
[64] This screenshot includes text translated by Telegram's translation function. Exhibit 1 includes the original message and a certified translation. *See* Ex. 1 at 74.

97. @wangduoyu0 often posts updates and advertisements for Lighthouse in this channel as well. For example, @wangduoyu0 posted an image of an investment account with a balance of almost $4 million, along with the note, "Hurry, contact me to buy a table and start fishing." I believe the "table" refers to Lighthouse and "fish" refers to victims of carding fraud.

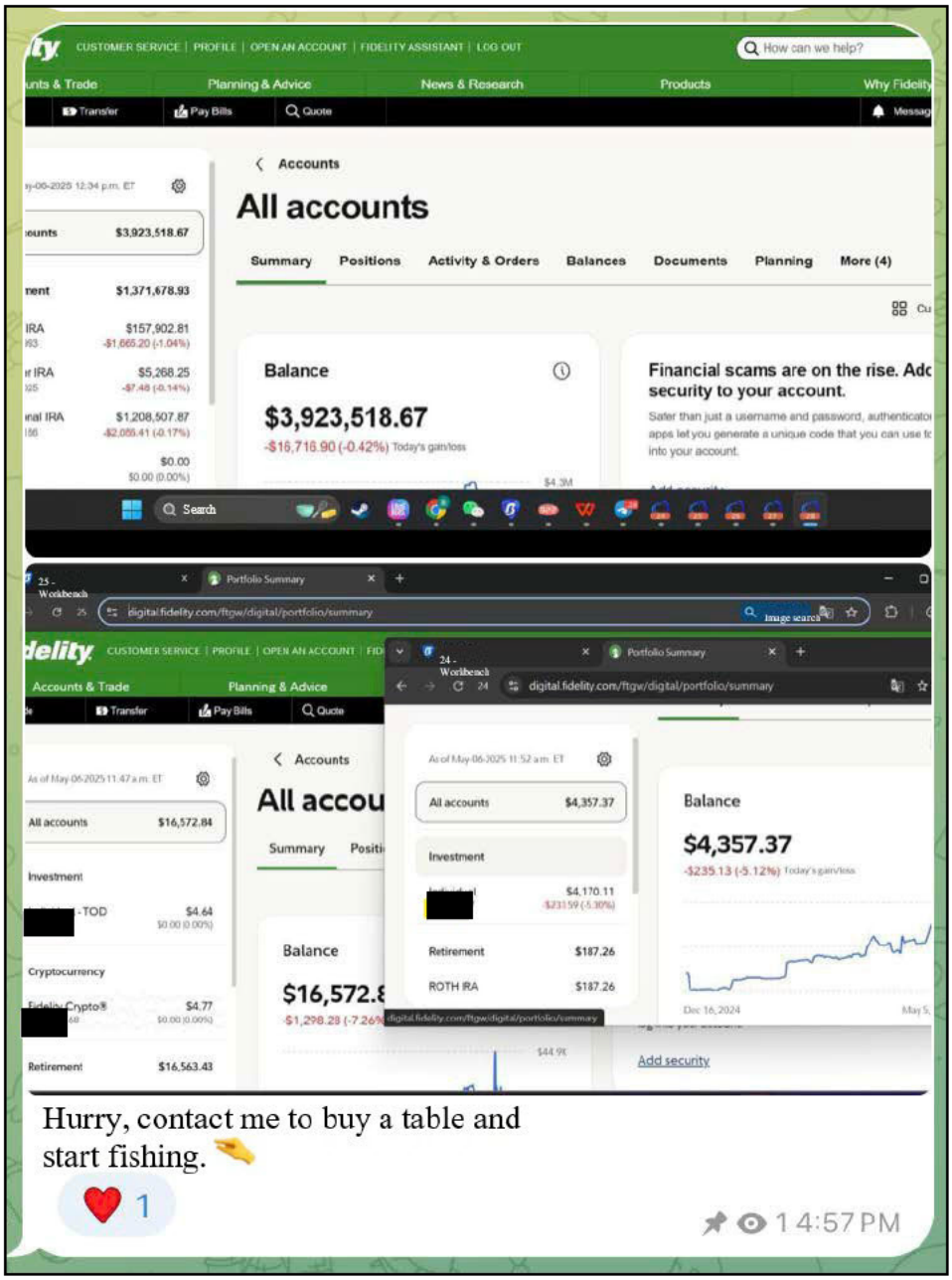


Figure 41. @wangduoyu0 Post in @laowanglive Telegram Group, https://t[.]me/laowangLiveGroup/1014 (translated)[65]

[65] Ex. 1 at 80.

98. In the same group, @wangduoyu0 posted screenshots of phishing templates available through the Lighthouse software. For example, on different dates in April 2025, @wangduoyu0 posted templates for fake login screens for three financial services companies.

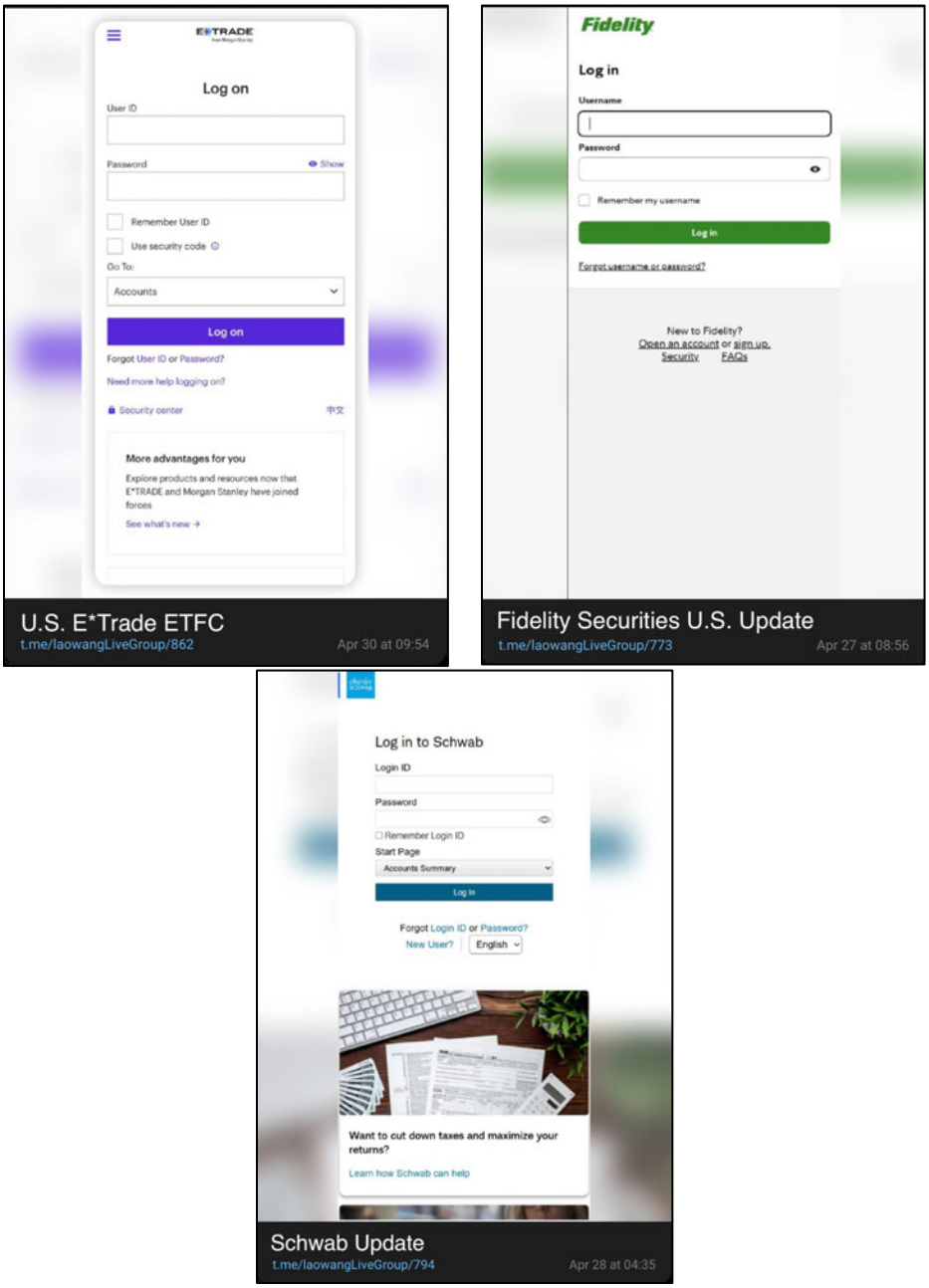


Figure 42. @wangduoyu0 Advertising Phishing Templates on Telegram, https://t[.]me/laowangLiveGroup/773, 794, 862 (translated)[66]

[66] Ex. 1 at 88–90.

99. @wangduoyu0 is one of seven administrators ("admins") of the @laowangLiveGroup.[67] Admins all have authority to invite, ban, or remove members or moderate content by deleting messages, "pinning" important messages, and controlling other chat settings. The group admins all apparently provide different services to support the Lighthouse phishing operation.

100. One admin with username @fyy8588 identifies himself or herself as "CoSmile." This user's profile contained a link to another known phishing forum cosmileonly[.]com, which the Telegram profile described as a forum that "helps those who are new to the C-world avoid detours and helps those who are lost find a warm home." CoSmile is the webmaster of that forum, *i.e.*, the website administrator. I know that the "C-world" is a term that often refers to "carding" or stealing credit card information. Wang Duo Yu is also active on the CoSmile forum, and on April 25, 2025, posted, "Hi everyone, I'm Duoyu! I've been involved in the C-circle for three years now without even realizing it. Thanks to the help of the site administrator, I've been able to achieve what I have today. My first significant earnings came from working with the site administrator, and that's how I met him."[68] I believe that "the site administrator" refers to CoSmile, who may have also helped Wang Duo Yu create Lighthouse.

101. CoSmile also operates a private channel of which @wangduoyu0 is a member and where @wangduoyu0 also advertises Lighthouse. For example, on May 14, 2025, @wangduoyu0 posted an advertisement for Lighthouse in that channel:

[67] There is one additional admin account but I have not included it as it is a bot used to manage numerous Telegram groups.

[68] This was posted by a username "Wang Duoyu" using the same avatar as the @wangduoyu0 Telegram profile and linking to the Telegram profile in their CoSmile bio. *See* Comment, @wangduoyu0, CoSmile (Apr. 25, 2025). Ex. 1 at 98–106.

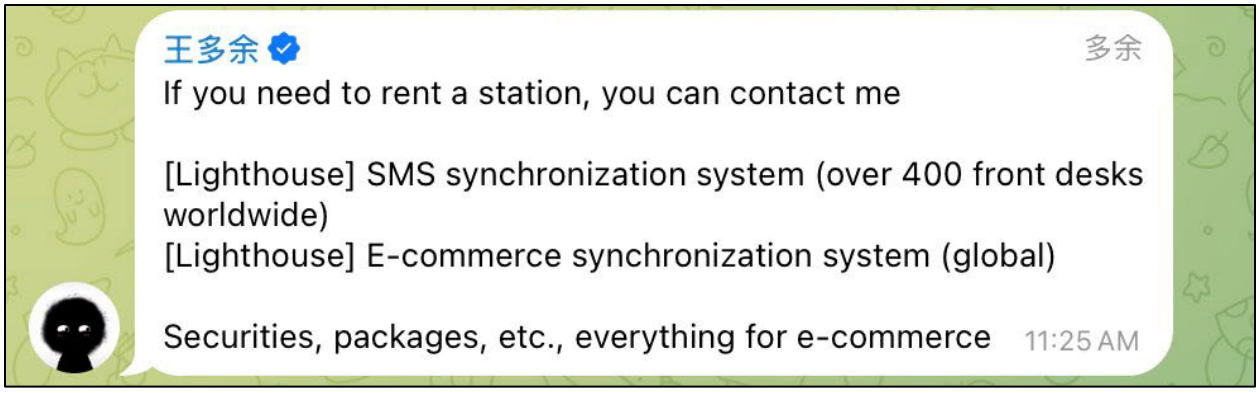


Figure 43. @wangduoyu0 Advertising Lighthouse on CoSmile's Private Channel, https://t[.]me/c/1544032714/443411 (translated)[69]

102. In addition, that same day, May 14, 2025, @wangduoyu0 and CoSmile had the following conversation in which they discussed @wangduoyu0 making tens of millions of dollars, likely from his phishing operation.

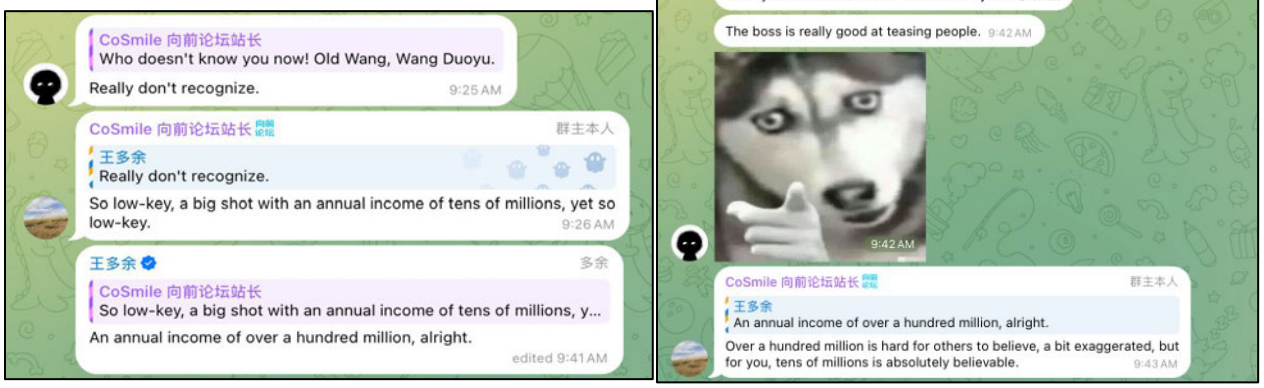


Figure 44. Screenshots of @wangduoyu0 and CoSmile Conversation, May 14, 2025, https://t[.]me/c/1544032714/443385 (translated)[70]

[69] This screenshot includes text translated by Telegram's translation function. Exhibit 1 includes the original message and a certified translation. *See* Ex. 1 at 110.
[70] This screenshot includes text translated by Telegram's translation function. Exhibit 1 includes the original message and a certified translation. *See* Ex. 1 at 118–120.

103. Another admin of the @laowangLiveGroup is a user with Telegram username @Gblockduouyu (a.k.a. Kunlun). This user is a "spammer" who provides bulk SMS sending services for Lighthouse users. @Gblockduoyu's profile reads, "RCS mobile phone room, daily sales of millions, multiple cooperation methods, quantity and price! Rental platform." As will be discussed in more detail below, @wangduoyu0 directs Lighthouse users to @Gblockduoyu for RCS services. In one post in the @laowangLiveGroup on July 17, 2025, @wangduoyu0 also referred to @Gblockduoyu as Lighthouse's "Official" RCS provider.

104. Another group admin @xiaobai77699 (a.k.a. Nutbrownbear) credits Wang Duo Yu as being their teacher in a post on the CoSmile forum from February 27, 2025. Specifically, Nutbrownbear wrote, "I entered the industry around 2022. My first pot of gold came through my mentor Duoyu Wang."[71] @xiaobai77699 also operates their own Telegram channel offering Lighthouse for sale. Below is an example of a post in that channel advertising Lighthouse from June 6, 2025.

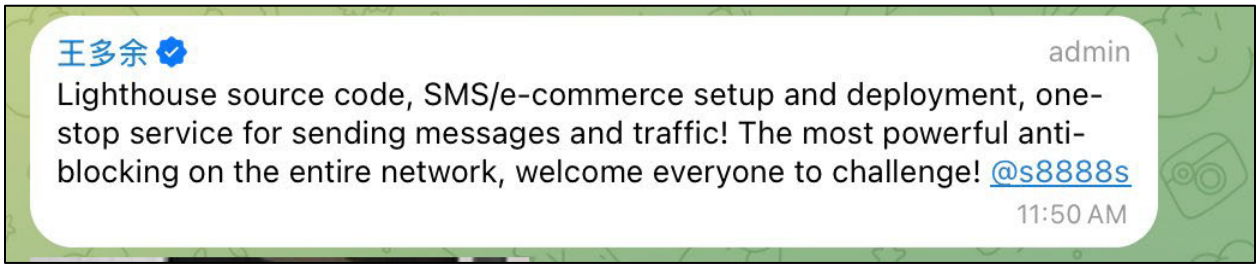


Figure 45. Promoting Lighthouse on @xiaobai77699's Channel on June 6, 2025, https://t[.]me/quanqiuwaimaijiaoliu/32930 (translated)[72]

105. Additionally, in one post in the same channel, on September 15, 2025, @xiaobai77699 offered escrow services as well as various links to other services related to phishing schemes provided by other users. Specifically, the post included a menu of referral

[71] *See* Blog Post, nutbrownbear (Feb. 27, 2025), *on* CoSmile. Ex. 1 at 128.
[72] This screenshot includes text translated by Telegram's translation function. Exhibit 1 includes the original message and a certified translation. *See* Ex. 1 at 136.

services: a link to the Lighthouse source code, a link to another @laowangLiveGroup administrator, @zldfgrw, who offers services to bulk buy tickets to global attractions, and a link to a user who is selling "[h]ijacked databases/accounts," *i.e.*, potential victims, from "various countries."

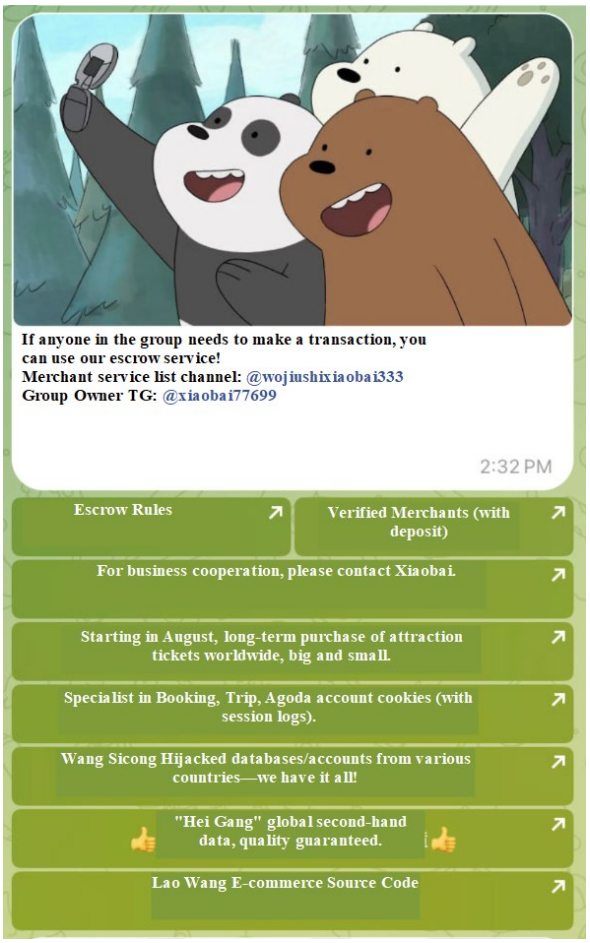


Figure 46. Services Related to Phishing Schemes Offered in @xiaobai77699's Channel, September 15, 2025, https://t[.]me/quanqiuwaimaijiaoliu/47003 (translated)[73]

106. @xiaobai77699 also offered to sell Lighthouse or to connect users to @wangduoyu0 on more than one occasion. In the same channel on April 19, 2025, @xiaobai77699 posted a picture of their "studio." I note that the studio appears to have six different computer stations set up, which is consistent with an organized cyber operation.

[73] Ex. 1 at 140.

Figure 47. Photo of @xiaobai77699's "Studio" Posted on April 19, 2025, https://t[.]me/quanqiuwaimaijiaoliu/23764

107. Another group admin, @zldfgrw, who goes by the name "August," advertises services of a business that allows for the purchase of large quantities of tickets to global attractions. In a now deleted post on @laowangLiveGroup on July 2, 2025, @zldfgrw wrote, "Seeking a professional and efficient agent to quickly reissue and purchase tickets from major tourist attractions worldwide."[74] I believe that this user likely offers a way to launder funds stolen through phishing. In @zldfgrw's bio, he or she wrote that Wang Duo Yu and others have already placed orders.

108. Admin @seven7zai, who goes by "Seven," also advertised services on @laowangLiveGroup that may be related to phishing. This user offered services including "snapping up goods and cashing them out" and described having over 200 employees and "store

[74] Message from August (@zldfgrw) to @laowangLiveGroup, Telegram (July 2, 2025). Ex. 1 at 144.

access to various platforms year-round."[75] He or she also noted the availability of a "[b]ase station leased for years," which I believe may refer to rentals of phishing software or tools.

109. The channel includes one other admin, @cooler_chengz, whose Telegram presence is minimal and does not result in any evidence that they offer services connected to phishing. Given the content of the channel and the services offered by the other admins, however, it is clear that at least most of them work together to promote Lighthouse and support the various phishing scams it facilitates.

110. Although members of the communication group discuss phishing openly with each other, @wangduoyu0 instructs people to message that account directly for questions about Lighthouse.

111. Therefore, beginning on July 14, 2025, at approximately 3:25 p.m., I initiated a direct message conversation with @wangduoyu0. The owner responded to my message within a minute and the following conversation ensued.[76]

[redacted]:[77]	My language is English. I am using a translator. Who should be paid for the software and license code?[78]
Wangduoyu0:	If you haven't received a response yet, please go to the Lighthouse Self-Service store to purchase the source code (new users click on top up and enter the amount) Self-service ordering at Lighthouse Store: @LighthouseShopBop
Wangduoyu0:	Pay me
Wangduoyu0:	TL8k7JY6KTU92HAVcCJcPAz2WTfFjSsYTZ
Wangduoyu0:	[Screenshot of QR Code of Cryptocurrency Address]

[75] Message from Seven (@seven7zai) to @laowangLiveGroup, Telegram (June 13, 2025). Ex. 1 at 148.
[76] *See* **Exhibit 2**, which is a true and correct copy of a certified translation of my conversation with @wangduoyu0 on Telegram.
[77] I communicated using a Telegram username that I have omitted from the declaration.
[78] I initially used Google Translate to communicate in Chinese.

Wangduoyu0: Trc20-usdt

Wangduoyu0: Which do you need to buy? E-commerce or SMS phishing source code?

[redacted]: SMS

[redacted]: How much?

Wangduoyu0: 199USD for one month. Permanent license is 2888usdt[79]

112. During our conversation, @wangduoyu0 directed me to the @LighthouseShopBot Telegram channel, an automated channel that appears to allow anyone with a Telegram account to purchase Lighthouse. I note that this channel is also described in @wangduoyu0's profile as "Self-service Order." @wangduoyu0 also directed me to send a payment in USDT and sent me a wallet address, which I will refer to herein as the TL8k7 address, based on the first five letters of the address. The user of @wangduoyu0 then provided me with prices for the SMS version of Lighthouse, a one-month license (199 USDT) and a permanent license (2888 USDT).

113. After that conversation, I told @wangduoyu0 that I needed time to get the USDT ready.[80] On July 16, 2025, and July 17, 2025, @wangduoyu0 followed up asking if I was ready to purchase yet.[81] On July 17, 2025, I sent @wangduoyu0 a link to a Telegram post in which someone had reported the TL8k7 address as a scam.[82] I expressed that I was concerned I might lose my money, and @wangduoyu0 responded by sending me screenshots of conversations with satisfied customers.[83] In one example, the customer claimed, "I have been doing fraud for like +- 4 years, I know you are probably millionaire by now and I really want to say thank you for finding time to

[79] Ex. 2 at 29.
[80] *Id.*at 31.
[81] *Id.*
[82] *Id.*
[83] *Id.*at 32–35, 42–46.

deal with me."[84] The @wangduoyu0 user responded "You're welcome. This is what I should do." The other conversations made clear that @wangduoyu0 provides "customer service" support to scammers after they purchase the software.[85] For example, in one conversation someone asked if they "can make an account for my friend to use in same time?" and @wangduoyu0 sent them a tutorial video.[86] In another conversation, @wangduoyu0 provided a customer with assistance setting up the software.[87]

114. On July 19, 2025, @wangduoyu0 followed up with a message to me saying, "Bro, do you still want to buy it?" and later in the conversation, "I am the source code author, you can trust me, I will not lie to you" along with a screenshot of the Lighthouse platform, the code, and our chat.[88]

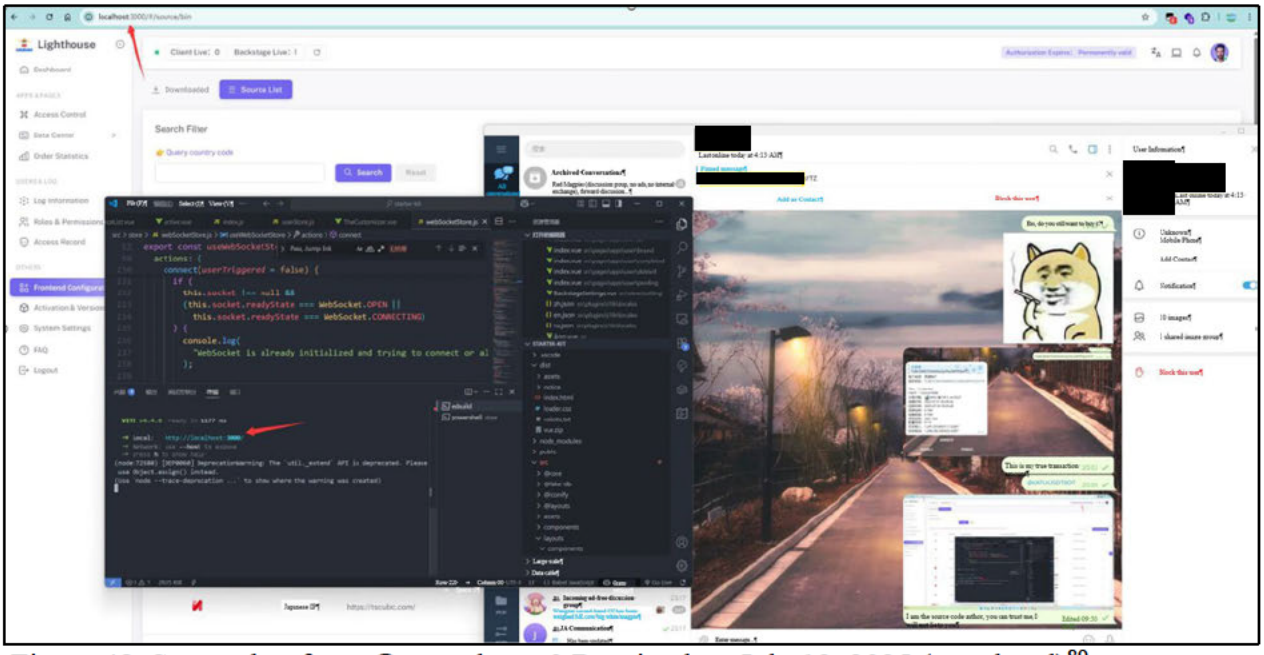


Figure 48. Screenshot from @wangduoyu0 Received on July 19, 2025 (translated)[89]

[84] *Id.* at 47.
[85] *Id.* at 42–47.
[86] *Id.* at 44.
[87] *Id.* at 47.
[88] *Id.* at 35, 49–50.
[89] *Id.* at 50.

115. @wangduoyu0 sent messages following up again pressuring me to buy on July 20, July 21, July 24, and August 7, 2025.[90] On August 14, 2025, we had the following conversation:

[redacted] Can you give me a trial license for a day or even a few hours so I know if I can successfully use it?

Wangduoyu0: No.

[redacted]**:** [Crying emoji.]

Wangduoyu0: Has a weekly card

Wangduoyu0: Week 188 USDT, Monthly 400 U, Permanent 1288 USDT

Wangduoyu0: See how you choose.

[redacted]**:** Can I at least get a WordPress setup tutorial before I pay?

Wangduoyu0: Cannot

[redacted]**:** Can I get a license for SMS and WordPress? Do you need to download two separately?

Wangduoyu0: Okay

Wangduoyu0: Two activation codes

Wangduoyu0: These are two prices.

Wangduoyu0: Permanent 2888u for SMS class
E-commerce 1288u

[redacted]**:** But only one download is required? Just one platform?

Wangduoyu0: Yes

[redacted]**:** Is it just a different template or is there other SMS-specific feature?

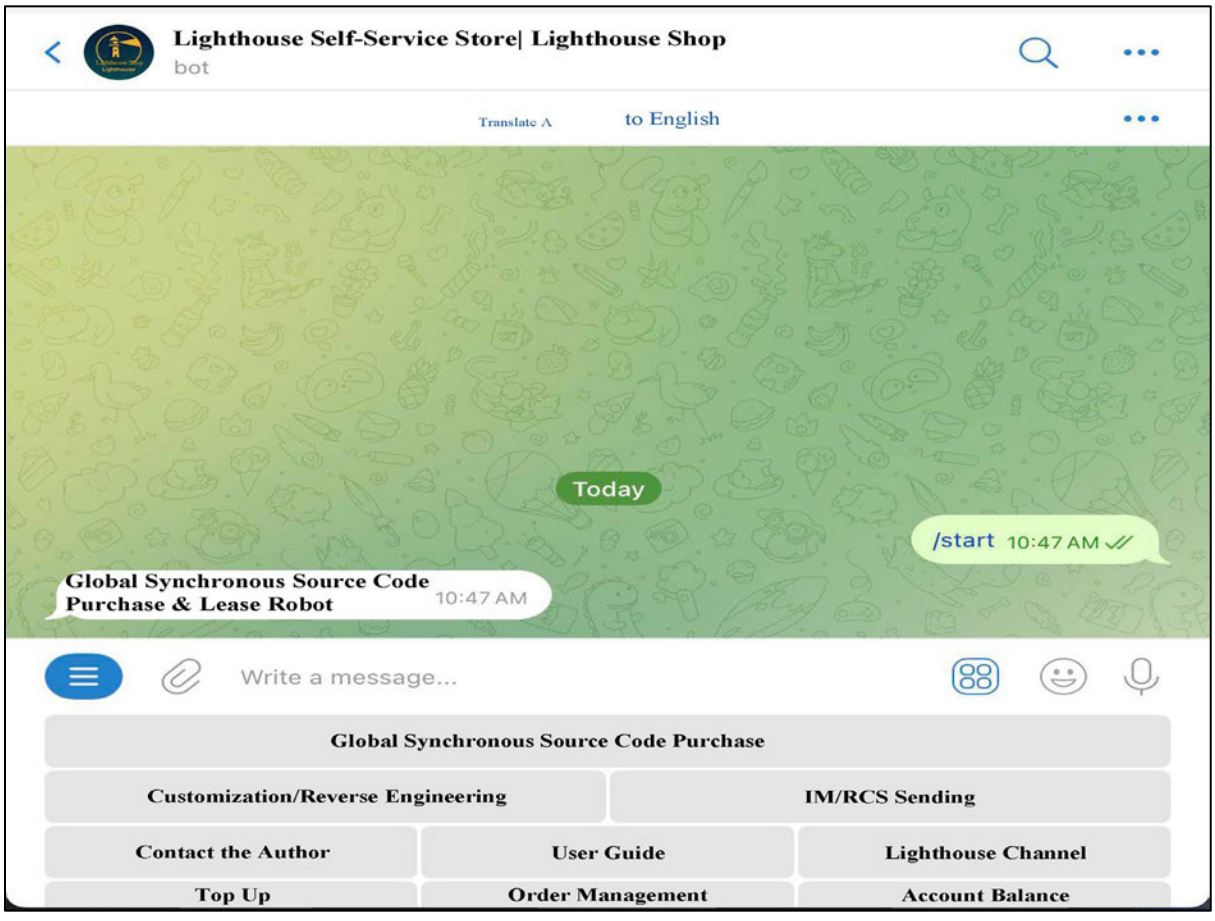
Wangduoyu0: SMS has the function of SMS

[90] *Id.* at 35–37.

Wangduoyu0: Different templates for SMS[91]

116. @wangduoyu0 clarified that the same software supports both the SMS and CMS versions of the tool, though different licenses are required. This is consistent with my review of the tool. I understand that with an SMS subscription, I would be able to use the SMS templates and unlock a feature of the software that allows the bulk sending of text messages.

117. I also reviewed the @LighthouseShopBot page on Telegram. Although I did not purchase the software through this page, I reviewed all of the menu options to understand how people typically make purchases. The following screenshots show the different purchasing options in this automated menu.[92]



[91] *Id.* at 39–40.
[92] Exhibit 3 depicts the menu options and process for ordering Lighthouse.

Figure 49. @LighthouseShopBot Telegram Channel Menu (translated)[93]

118. I clicked on "Global Synchronous Source Code Purchase" and was brought to a page that allowed me to choose between "SMS Sync System" and "Ecommerce Sync System." After clicking on the option for SMS Sync System, I was brought to a page that listed pricing for different licensing terms (*e.g.*, weekly, monthly, and permanent). The prices are consistent with those that @wangduoyu0 quoted to me in our Telegram conversation.

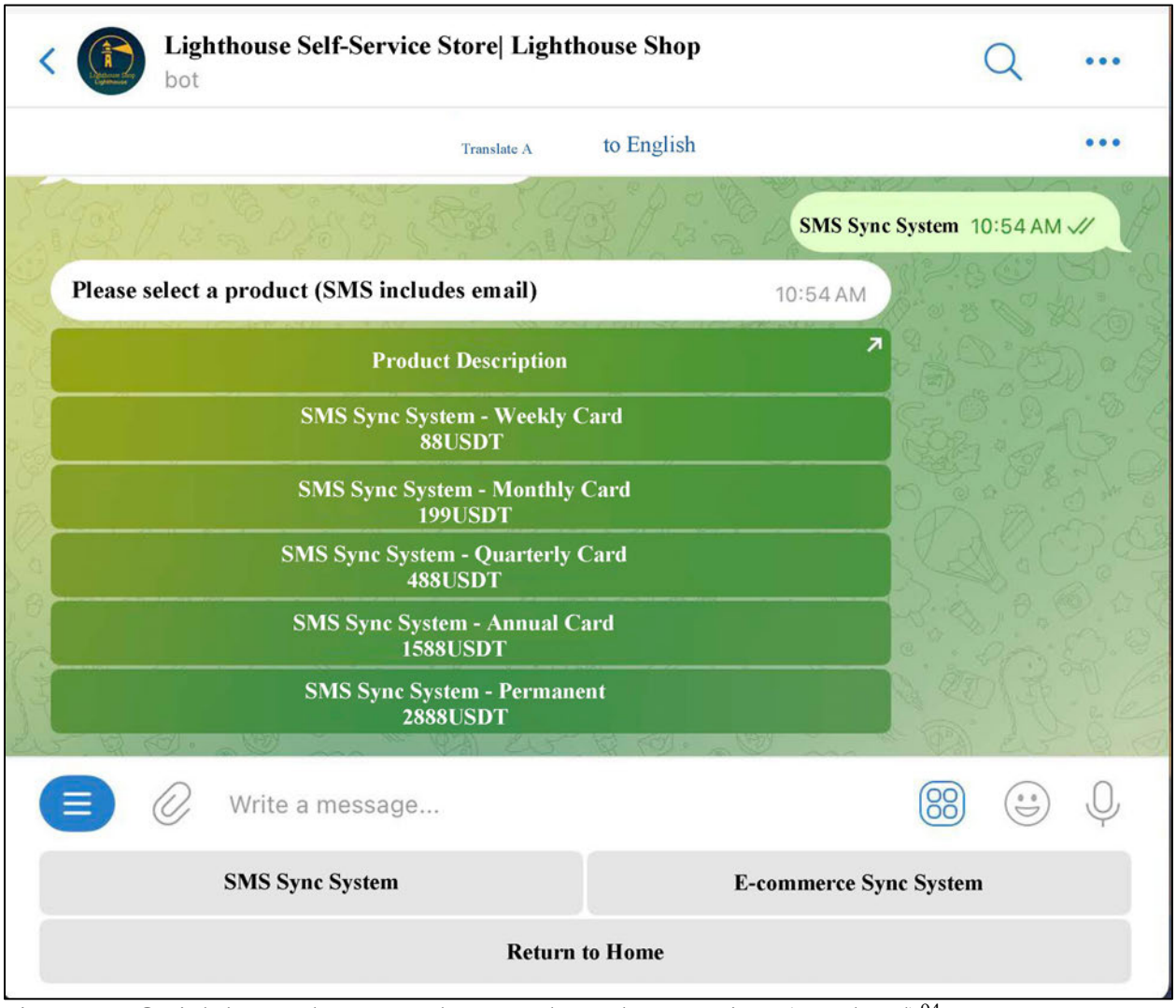


Figure 50. @LighthouseShopBot Telegram Channel SMS Prices (translated)[94]

[93] Ex. 1 at 152.
[94] Ex. 1 at 156.

119. Choosing any of the license options led me to a page that read, "insufficient balance: 0 USDT. Please recharge before making a purchase." I navigated back through the menu to choose the e-commerce options and was given the choice between the Chinese e-commerce platform synchronization system and the CMS synchronization system. The menu similarly took me through various purchasing options. I prepared a chart to summarize the various licensing options for sale through the @LighthouseShopBot channel.

Product Type	License Length	Price (USDT)
SMS	Permanent	2888
SMS	Annual	1588
SMS	Season	488
SMS	Monthly	199
SMS	Weekly	88
Ecommerce WordPress Stripe	Permanent	1288
Ecommerce WordPress Stripe	Monthly	400
Ecommerce WordPress Stripe	Weekly	188
Ecommerce WordPress PayPal	Permanent	1388
Ecommerce WordPress PayPal	Monthly	400
Ecommerce WordPress PayPal	Weekly	188
Ecommerce WordPress Stripe AND PayPal	Permanent	2388
Ecommerce WordPress Stripe AND PayPal	Monthly	688
Ecommerce WordPress Stripe AND PayPal	Weekly	288
Ecommerce SHOPYY Without Store Prices	Permanent	2888
Ecommerce SHOPYY Without Store Prices	Monthly	498
Ecommerce SHOPYY Without Store Prices	Weekly	198
Ecommerce SHOPYY With Store Prices	Monthly	598
Ecommerce SHOPYY With Store Prices	Weekly	198

Figure 51. @LighthouseShopBot Pricing

120. I navigated back to the main menu (Figure 49). I noted that when choosing "Customization/Reverse Engineering" and "Contact the Author" I was directed to contact @wangduoyu0. When choosing either "User Guide" or "Lighthouse Channel" I was redirected to the @laowang_notice channel.

121. When choosing "IM/RCS Sending" I was directed to a message that stated "RCS Terminal Room" and linked me to one of @wangduoyu0's partners. The Telegram page referenced "multiple cooperation methods, volume-based pricing, absolutely real." It also claimed that it facilitated "millions of connections daily." It then listed various countries that the messages could be delivered to, including the United States. The channel then offered users the ability to send a

message to Telegram user @Gblockduoyu. I understand this to mean that @wangduoyu0 offered the service of connecting users to a trusted partner, @Gblockduoyu, who handled sending the messages necessary to contact victims of the SMS scam. I know that sending out millions of text messages is an operation that requires various people, who often operate as many as hundreds of cellular telephones. By integrating the ability to contact @Gblockduoyu into the Lighthouse Shop Bot page, @wangduoyu0 was able to link customers with a trusted partner and incorporate this service into Lighthouse.

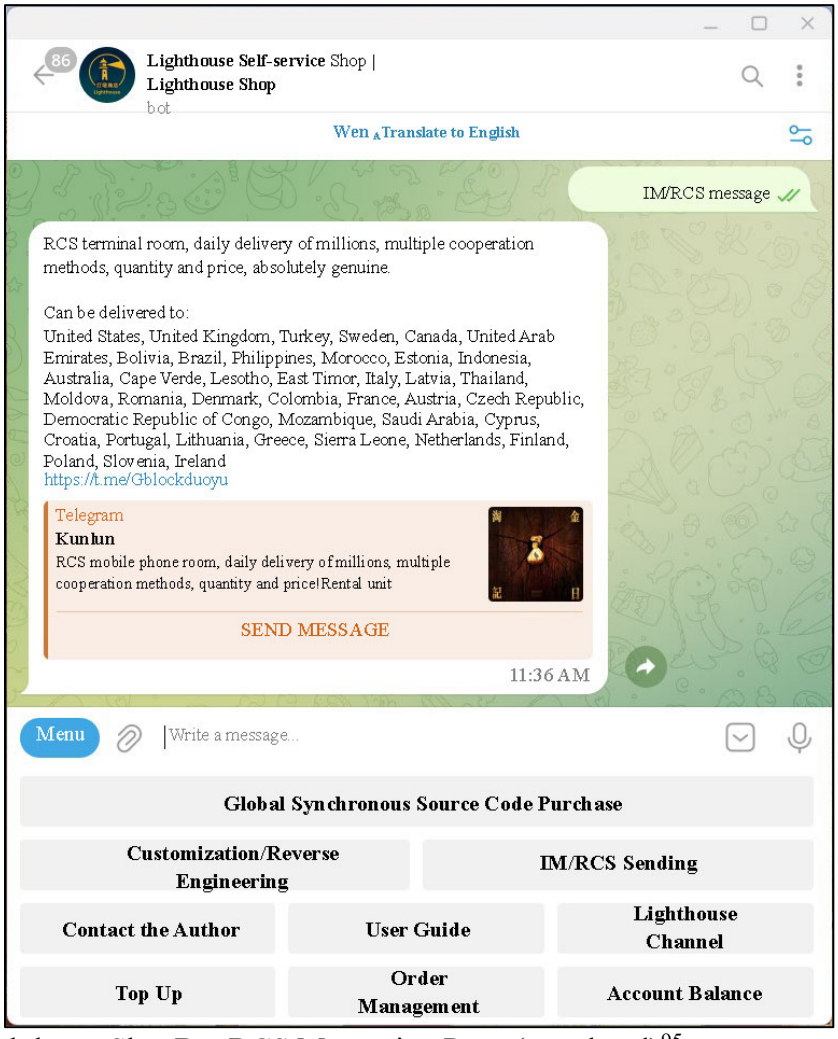


Figure 52. @LighthouseShopBot RCS Messaging Page (translated)[95]

[95] This screenshot was taken using the Telegram translation feature. A certified translation is included in Exhibit 1, see page 160.

122. After navigating back to the @LighthouseShopBot main menu and choosing the option to "Top Up," I was provided with a different cryptocurrency address that I will refer to as the TXnmg address.

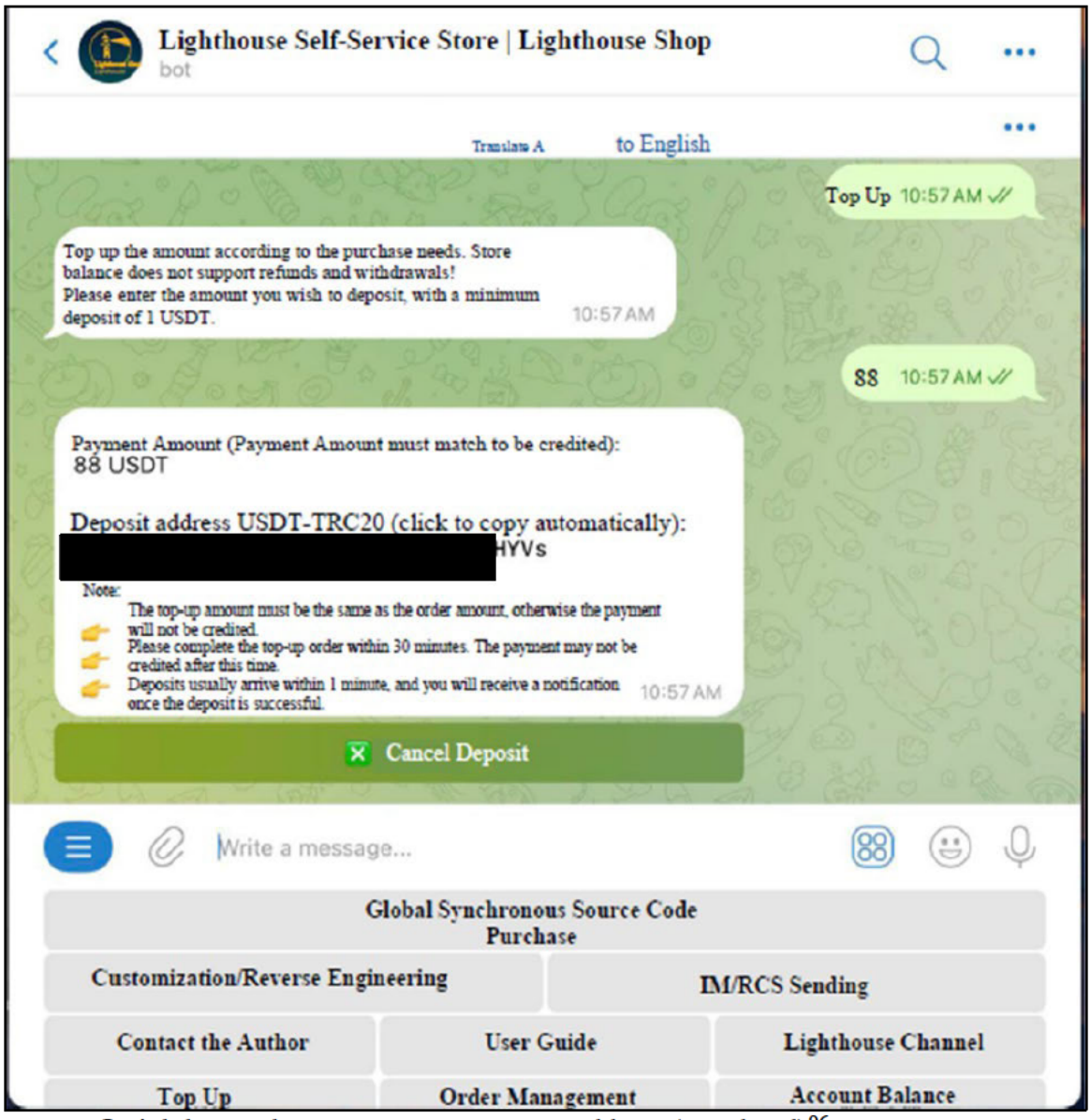


Figure 53. @LighthouseShopBot USDT Payment Address (translated)[96]

123. I believe that @wangduoyu0 used the TXnmg address and the TL8k7 address to receive payment in USDT for Lighthouse licenses.

[96] Ex. 1 at 164.

VI. Conclusions

124. Lighthouse is a comprehensive phishing tool that uses deceptive practices and techniques specifically designed to defraud individual victims and financial institutions. @wangduoyu0 (a.k.a. Wang Duo Yu), @fyy8588 (a.k.a. CoSmile), @Gblockduoyu (a.k.a. Kunlun), @xiaobai77699 (a.k.a. Nutbrownbear), and others distribute the phishing software through an organized communication and payment platform that advertises features, provides updates, and assists "customers" with technical issues.

125. By impersonating government agencies and trusted companies to steal from victims, these fraudsters erode the trust everyday users place in these institutions and the internet. Given the software's customization features, no company is safe from potential impersonation, and no internet user is safe from being targeted. Phished information not only leads to individual financial losses, but it can also be the entry point for ransomware and innumerable other cyber-attacks. The technical complexity and versatility of Lighthouse along with the sophisticated and broad network of cybercriminals supporting Lighthouse phishing schemes make this phishing-as-a-service network particularly dangerous.

In accordance with 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Executed on November 11, 2025 in [redacted]

[redacted]