UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	Hon. James B. Clark, III
	:	
v.	:	Mag. No. 24-12280
	:	
REMINGTON GOY OGLETREE, a/k/a "remi"	:	**CRIMINAL COMPLAINT**

I, Andrew Feiter, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

I further state that I am a Special Agent with the Federal Bureau of Investigation, and that this complaint is based on the following facts:

SEE ATTACHMENT B

continued on the attached page and made a part hereof.

s/*Andrew Feiter*
Special Agent Andrew Feiter
Federal Bureau of Investigation

Special Agent Feiter attested to this Complaint by telephone pursuant to FRCP 4.1(b)(2)(A).

Sworn to and subscribed via telephone, this 30th day of October, 2024

NEW JERSEY
State

HONORABLE JAMES B. CLARK, III
UNITED STATES MAGISTRATE JUDGE

Signature of Judicial Officer

ATTACHMENT A

COUNT ONE
(Wire Fraud)

From in or around October 2023 through in or around May 2024, in Hudson County, in the District of New Jersey and elsewhere, defendant

REMINGTON GOY OGLETREE,
a/k/a "remi"

knowingly and intentionally devised and intended to devise a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing and attempting to execute such scheme and artifice to defraud, did transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, to wit, a wire transmission sent on or about October 10, 2023, from a location outside of New Jersey to a location inside of New Jersey.

In violation of Title 18, United States Code, Section 1343 and Section 2.

COUNT TWO
(Aggravated Identity Theft)

On or about October 10, 2023, in the District of New Jersey and elsewhere, defendant

REMINGTON GOY OGLETREE,
a/k/a "remi"

knowingly transferred, possessed, and used, without lawful authority, a means of identification of another person during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), to wit, wire fraud, in violation of Title 18, United States Code, Section 1343, knowing that the means of identification belonged to another actual person, specifically the username and password of a Telecom Business-1 employee ("Employee-1").

In violation of Title 18, United States Code, Section 1028A(a)(1) and Section 2.

ATTACHMENT B

1. I, Andrew Feiter, a Special Agent with the Federal Bureau of Investigation ("FBI"), having personally participated in an investigation of the conduct of defendant REMINGTON GOY OGLETREE, a/k/a "remi," ("OGLETREE"), and having spoken with other law enforcement officers and individuals and reviewed documents, have knowledge of the following facts. Because this Complaint is submitted for the limited purpose of establishing probable cause, I have not included all facts known to me concerning this investigation. The contents of documents and the actions, statements, and conversations of individuals referenced below are provided in substance and in part, unless otherwise indicated. Similarly, dates and times are approximations, and should be read as "on or about," "in or about," or "at or about" the date or time provided.

Introduction

2. The FBI is investigating a group of criminal cyber actors ("the Cyber Threat Group") and their associates who access victim companies' computers and networks without authorization, encrypt victim companies' data and/or exfiltrate that data to an offsite device, and extort virtual currency from the victim companies in order for them to regain control over their computers and data. The Cyber Threat Group has been referred to as "Scattered Spider," "Octo Tempest," "UNC3944," and/or "0ktapus". The Cyber Threat Group has targeted victims throughout the United States, including in New Jersey.

3. The investigation into the Cyber Threat Group has revealed that from at least October 2023 through at least May 2024, OGLETREE perpetuated a scheme to defraud in which he called and sent phishing messages to U.S.- and foreign-based company employees to gain unauthorized access to the companies' computer networks. Once OGLETREE had access to the victim companies' networks, OGLETREE accessed and stole confidential data, including data that was later posted for sale on the dark web, and, at times, used the companies' services to facilitate the theft of cryptocurrency from unwitting victims. As a result of OGLETREE's scheme, victims have suffered over $4 million in losses.

Relevant Individuals and Entities

4. At various times relevant to this Complaint:

   a. OGLETREE was a resident of Florida and Texas.

   b. Telecom Business-1 was a U.S.-based telecommunications company that offered a communications platform as a

service that provides voice, messaging, and other communication services through its cloud-based platform.

c. Financial Institution-1 was a U.S.-based national bank.

d. Telecom Business-2 was a Europe-based telecommunications company that provided voice, messaging, and other communication services through a cloud-based platform.

Definitions

5. I know from my training, experience, and research as a Special Agent with the FBI that the following definitions apply to the activity discussed in this affidavit:

a. **Domain**: A domain (short for domain name) is a website's electronic address on the Internet. Examples include www.justice.gov and www.uscourts.gov. Domains are used to help users navigate to websites more easily instead of having to use the site's IP address.

b. **Registration**: "Registration" is the act of reserving a domain on the Internet for a specific time period. In order to do so, the "domain registrant" would usually apply online to a company that managed the reservation of Internet domain names, known as a registrar. A "registrar" operates in accordance with the guidelines of the designated organizations that manage top-level domains (e.g., ".com" or ".net"), known as registries.

c. **Cryptocurrency**: "Digital currency" or "virtual currency" is currency that exists only in digital form; it has the characteristics of traditional money, but it does not have a physical equivalent. Cryptocurrency, a type of virtual currency, is a network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Bitcoin ("BTC") and ether ("ETH") are examples of cryptocurrency. Cryptocurrency can exist digitally on the internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys can be printed or written on a piece of paper or other tangible object.

Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Most cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.

d. **Private Key**: A private key is a cryptographic key that is uniquely associated with an entity and not made public. In the blockchain and virtual currency context, virtual currency addresses are controlled using a unique corresponding private key, the equivalent of a password, which is needed to access the funds associated with the address. Only the holder of an address's private key can authorize a transfer of virtual currency from that address to another address.

e. **Public Key**: A public key is a cryptographic key that is uniquely associated with a person or entity and is designed to be made public. The public key is paired with, and derived from, a private (secret) key. However, knowing the public key does not reveal any information about the private key. In the blockchain and virtual currency context, a virtual currency address is the hashed value of a public key and acts as an identifier on a blockchain.

f. **Cryptocurrency wallet**: A cryptocurrency wallet is an application that holds a user's cryptocurrency addresses and private keys. A cryptocurrency wallet also allows users to send, receive, and store cryptocurrency. Multiple virtual currency addresses can be controlled by one wallet.

g. **Hardware Wallet**: A hardware wallet is a physical, removable device that stores a user's private keys and can be connected to a computer when a user wishes to use the keys stored on the wallet for virtual currency transactions. Hardware wallets can be secured with PINs and passphrases and can be backed up or regenerated with a recovery phrase. Trezor is an example of the type of hardware wallets on the market.

h. **Hosted Wallet**: A hosted wallet, also known as a custodial wallet, is a virtual currency wallet through which a third party, e.g., a virtual currency exchange, holds a user's private keys. The third party maintains the hosted wallet on its platform akin to how a bank maintains a bank account for a customer, allowing the customer to authorize virtual currency transactions involving the hosted wallet only by logging into/engaging with the third party's platform.

i. **Blockchain**: A blockchain is a digital ledger run by a decentralized network of computers referred to as "nodes." Each node runs software that maintains an immutable and historical record of every transaction utilizing that blockchain's technology. Many digital assets, including virtual currencies, publicly record all of their transactions on a blockchain, including all of the known balances for each virtual currency address on the blockchain. Blockchains consist of blocks of cryptographically signed transactions, and blocks are added to the previous block after validation and after undergoing a consensus decision to expose and resist tampering or manipulation of the data. There are many different blockchains used by many different virtual currencies. For example, Bitcoin in its native state exists on the Bitcoin blockchain, while Ether (or "ETH") exists in its native state on the Ethereum network.

j. **Blockchain Analysis**: Law enforcement can trace transactions on blockchains to determine which virtual currency addresses are sending and receiving particular virtual currency. This analysis can be invaluable to criminal investigations for many reasons, including that it may enable law enforcement to uncover transactions involving illicit funds and to identify the person(s) behind those transactions. To conduct blockchain analysis, law enforcement officers use reputable, free open source blockchain explorers, as well as commercial tools and services. These commercial tools are offered by different blockchain-analysis companies. Through numerous unrelated investigations, law enforcement has found the information associated with these tools to be reliable.

k. **Server**: A server is a computer or operating system that provides resources, data, services, or programs to other computers (commonly referred to as "clients") over a

network. There are many types of servers, including web servers that provide content to web browsers, email servers that act as a post office to send and receive email messages, print servers, virtual private servers, and proxy servers.

l. **VPS**: A virtual private server ("VPS") is a virtual operating system that resides within a physical parent server and uses virtualization technology to provide dedicated, private resources to other servers. A VPS runs its own copy of an operating system, and customers can have access to that operating system to install almost any software that runs on that operating system. For many purposes, a VPS is functionally equivalent to a dedicated physical server but, being software-defined, can be created and configured more easily. Many companies offer virtual private server hosting or virtual dedicated server hosting as an extension for web hosting services.

m. **Phishing**: Phishing is a cyber-attack technique where the attacker sends a message to lure the recipient into clicking on a link (often to a website or program) and then provide sensitive information or download malicious software on to the recipient device. SMS phishing refers to a type of phishing that uses text messages, which are commonly sent over SMS (Short Message Service) channels but also can be sent using non-SMS channels like data-based messaging applications.

n. **Phishing website**: A phishing website is a website that is designed to appear like it is associated with a legitimate company or organization for the purpose of luring the victim into opening the website and/or providing sensitive information through the website. Phishing websites commonly have domain names that are similar to the domain names of the legitimate company or organization that they are trying to imitate.

o. **Social engineering**: Social engineering refers to deceptive techniques that are designed to convince another person to reveal specific information or perform a specific action when the perpetrator would not otherwise have access to that information or action. Phishing is a type of social engineering technique.

p. **Cookies**: "Cookies" are pieces of data used to save information relating to a computer user and his or her preferences. Providers such as Google use cookies and similar technologies to track users visiting Google's webpages and using its products and services. Using this technology, Google may be able to identify two accounts as "linked by cookie" if the same internet browser was used to access both accounts.

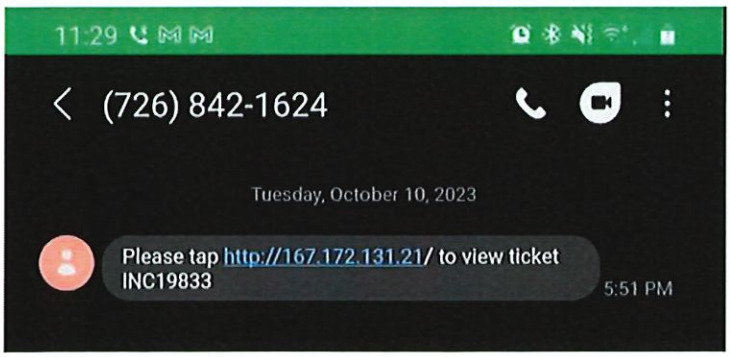
q. **API**: API, which stands for Application Programming Interface, is a set of protocols and definitions that allow technology products and services to communicate with each other. An API "key" is a unique identifier and secret token used to authenticate an application or user of an API.

r. **Splashtop**: Splashtop is a remote desktop software platform that allows users to access and control computers from a remote location over the internet and can be used to transfer files between computers. Splashtop has been used in network intrusions to gain remote control of a system, maintain persistence in a system, and remove data.

Cyber Intrusion 1

6. In or around October 2023, Telecom Business-1 became aware of an unauthorized access to several of its applications and systems. According to information provided by Telecom Business-1, the perpetrator gained access through a phishing campaign targeting Telecom Business-1 employees.

7. Specifically, on October 10, 2023, a U.S.-based Telecom Business-1 employee ("Employee-1") received a phone call from an individual impersonating Telecom Business-1 information technology ("IT") support. The caller pressured Employee-1 to access a link the caller sent via the following phishing text:



8. Employee-1, who was not located in the state of New Jersey at the time, clicked the link and provided his Telecom Business-1 username and password believing he was following the instructions of Telecom Business-1's IT support. Employee-1's username and password were then harvested and used to access Telecom Business-1's network. The domain used to harvest Employee-1's credentials was hosted on IP Address 167.172.131.21 (the "21 IP Address"). According to records provided by the company hosting the 21 IP Address, the 21 IP Address is hosted on a server located in New Jersey.

9. Once inside Telecom Business-1's network, the perpetrator, believed to be OGLETREE for the reasons set forth below, gained access to and stole confidential company data, including customer API keys. Telecom Business-1's API enabled customers to integrate voice calling and texting capabilities into applications and allowed management of inbound and outbound calls and texts. The perpetrator used the API keys to access and use multiple Telecom Business-1 customer accounts. The perpetrator then used those customer accounts to send and attempt to send approximately 8.5 million phishing texts to phone numbers across the nation, including to phone numbers with New Jersey area codes. The phishing text messages included the following messages designed to steal cryptocurrency from individuals:

- 10/11/23 – "Your [Cryptocurrency Company-1] Earn balance is now available to withdraw at your[Cryptocurrency Company-1]claims.net"

- 10/12/23 – "[Cryptocurrency Company-2] You have received a trading fee reimbursement! Claim your USDT now at [Cryptocurrency Company-2]hub.com"

- 10/12/23 – "[Cryptocurrency Company-2] You have received a trading fee reimbursement. Claim your USDT now! [Cryptocurrency Company-2]claims.com"

- 10/12/23 – "[Cryptocurrency Company-2] You have received a trading fee reimbursement! Claim your USDT now at [Cryptocurrency Company-2]fees.com"

10. Telecom Business-1 provided records of the 8.5 million texts. The texts identified as their sender either: (a) one of six short code "sent" phone numbers (five digits instead of a 10-digit phone number); or (b) Cryptocurrency Company-2. A court-authorized search of an iCloud account used by OGLETREE (the "OGLETREE iCloud Account") revealed text messages that the OGLETREE iCloud Account received from three of the six short code numbers during the

Telecom Business-1 intrusion. Specifically, the OGLETREE iCloud Account received the following text messages:

- Received from short code 22044:
  - 10/11/23 - "Your [Cryptocurrency Company-1] Earn balance is now available to withdraw at your [Cryptocurrency Company-1]claim.net"
  - 10/11/23 – "acewarecwar"
  - 10/11/23 – "Your [Cryptocurrency Company-1] Earn balance is now available to withdraw at wavewavrewar.com"

- Received from short code 33021:
  - 10/11/23 – "[Video gaming company-1] You have rewards available to claim at https://[variation on Video gaming-company-1]"
  - 10/12/23 – "aewvrwaerva"
  - 10/12/23 – "[Cryptocurrency Company-2] You have received a trading fee reimbursement! Claim your USDT now at [Cryptocurrency Company-2]claims.com"
  - 10/12/23 – "Your [Cryptocurrency Company-1] Earn balance is available to withdraw at get[Cryptocurrency Company-1]earn.com"

- Received from short code 70222:
  - 10/12/23 – "wearwearb."
  - 10/12/23 – "[Video gaming company-1] You have unclaimed rewards! Visit https:// ://[variation on Video gaming-company-1] for more info."
  - 10/12/23 – "[Cryptocurrency company-1] You have received a trading fee reimbursement. Claim your USDT now! [Cryptocurrency company-1]fees.com"

11. Based on this investigation and my training and experience, I believe that the above text messages are evidence of OGLETREE having access to Telcom Business-1's network, using the API keys, and testing certain phishing messages before transmitting them to potential victims. For example, the texts "acewarecwar" and "wearwearb" appear to be random sequences of letters typed on a keyboard. In my training and experience, the timing of the transmittal of random letters to OGLETREE's phone further indicates that he was sending messages of random letters to himself to test the phishing messages.

12. According to Google records, Telecom Employee-1's credentials were linked by cookie with the email account zuiydacheater@gmail.com (the "Zuiydacheater Account"), indicating that the same internet browser was used to access both the "Zuiydacheater Account" and Employee-1's Telecom Business-1 account. As set forth below, OGLETREE admitted in an interview with the FBI that the Zuiydacheater Account belongs to him. Further, a court-authorized search of the Zuiydacheater Account revealed evidence indicating that OGLETREE owned the account. For instance, the username on the Zuiydacheater Account is "Remington Ogletree" and the account received emails to that name.

13. According to Apple records, the OGLETREE iCloud Account was subscribed to by "Steven Durango" at a Key Largo, Florida address (the "Key Largo Address") and phone number ending in 7923 (the "7923 Phone Number"). As described in more detail below, the Key Largo Address was an Airbnb where OGLETREE and his father stayed in late 2023. A public record check revealed that no person by the name of Steven Durango lives in Key Largo, Florida. Further, the 7923 Phone Number is registered to OGLETREE's father, and OGLETREE later admitted in an interview with the FBI that it was his own number. Evidence within the OGLETREE iCloud Account, including photos of OGLETREE and emails to OGLETREE, further shows that the account was used by OGLETREE during the relevant period. Finally, OGLETREE is listed as a billing contact for the OGLETREE iCloud Account.

14. The 7923 Phone Number appears 14 times in Telecom Business-1's records of the phishing texts sent between October 11-12, 2023, during the Telecom Business-1 intrusion. Multiple times, the first (or one of the first) texts from a particular number was sent to the 7923 Phone Number, suggesting, again, that OGLETREE was testing phishing messages by sending them to his own phone.

15. Data contained within the OGLETREE iCloud Account further reflects that OGLETREE received a phishing text impersonating Telecom Business-1 on October 7, 2023. The text message stated: "Your work schedule for next week has changed" and provided a web address impersonating Telecom Business-1. OGLETREE was not an employee of Telecom Business-1 at the time. This text is further evidence of OGLETREE testing phishing messages prior to sending them.

Cyber Intrusion 2

16. In or around October 2023, Financial Institution-1 observed an unauthorized access to its computer network. Financial Institution-1 reported that approximately 149 Financial Institution-1 employees received phishing text

messages directing them to phishing websites impersonating Financial Institution-1. Through those websites, the employees were directed to enter their Financial Insitution-1 credentials.

17. According to information provided by Financial Institution-1, the phishing text messages were received by Financial Instutiton-1 employees from as early as October 27, 2023 through November 16, 2023. A review of screenshots of the phishing messages revealed statements intended to mislead the employees into providing their credentials, including fraudulent messages claiming their "employee benefits package [was] updated" and "your employee schedule has been modified." Some of the phishing messages told employees that they had "an inquiry from HR" or that their "VPN profile was updated." The phishing messages directed the employees to click on a phishing link, which would direct them to a phishing website where they were prompted to provide their employee credentials.

18. While in New Jersey, on November 16, 2023, a New Jersey-based Financial Institution-1 employee received one of the phishing text messages. Specifically, the text contained a phishing link and claimed the employee's "VPN profile was updated."

19. Many of the phishing domains used as part of the Financial Institution-1 intrusion were hosted by Namecheap, a domain name registrar and web hosting company. According to Namecheap records, the phishing domains were registered to the following registrant usernames and email accounts, most of which appear to include random sequences of letters typed on a keyboard:

- SFawerwaer Awaverwer (AaweroijaEvw@ag.prout.be)
- Ryan Donlin (Avjoawvier123@hunnur.com)
- Ryan Donlin (jkrweavoij@tweet.fr.nf)
- Svrewa tvreaacwer (Namcheeap1337@bmn.ch.mavawerivjoaw @ag.prout.be)
- SDfwervawer Avawqeawer (vawerivjoaw@ag.prout.be)
- waerawverawe xzvrvwaer (Zvwearawer@ag.prout.be)
- Markis Timmons (zweaorviajw@yaloo.fr.nf)
- Sawevrwear Aawervwaer (ZZvoijafawer@ag.prout.be).

20. According to Namecheap records, the "Svrewa tvreaacwer" Namecheap account, which was used to register at least three phishing domains used in the Financial Company-1 intrusion, was created from IP address 185.156.46.163 (the "163 IP Address") on October 28, 2023, at 16:11:43 UTC.

21. Records provided by a video gaming company ("Video Gaming Company-1") reflect that an account was registered with Video Gaming

Company-1 using the email address zuiydacheater@yadim.dismail.de (as discussed above, OGLETREE also used "zuiydacheater" as the username for his Google email account) and the player name "remi" (the "Remi Video Gaming Account"). A review of purchase history records for the Remi Video Gaming Account revealed that the account's user made purchases in the name of "Remington Ogletree" using the Key Largo Address as a billing address from November 15, 2023, to November 28, 2023. Video Gaming Company-1 products are generally downloaded, and thus are not delivered to the physical address. Nonetheless, users are asked to provide an address when making purchases. According to Airbnb records, the residence located at the Key Largo Address was rented through Airbnb using an account held by OGLETREE's father. OGLETREE further received a confirmation email from Airbnb for this rental at one of his personal email accounts that was saved to the OGLETREE iCloud Account. The Airbnb rental began on October 18, 2023, was for 31 nights (or until November 18, 2023), and cost a total of approximately $25,070. According to Video Gaming Company-1 records, the 163 IP Address was also used to access the Remi Video Gaming Account on October 28, 2023, from 15:52 UTC to 22:25 UTC. The 163 IP Address, therefore, was used on the same day to access both the Remi Video Gaming Account and a Namecheap account used in furtherance of the Financial Company-1 intrusion.

22. A review of IP logs associated with the Financial Institution-1 intrusion revealed an unauthorized access from IP address 146.70.171.97 (the "97 IP Address") at 06:02:16 UTC on October 29, 2023. Namecheap records indicate that the Ryan Donlin (Avjoawvier123@hunnur.com) account, which was used to register phishing domains as explained above, was created from the 97 IP Address on October 29, 2023.

23. A review of records provided by Financial Insitution-1 further revealed that at least 14 of the phone numbers used to send phishing text messages to Financial Institution-1 employees were sent from a single Telecom Business-1 account. Telecom Business-1 records reveal the account was registered to a California resident ("Individual-1). According to Individual-1, he did not authorize the use of the Telecom Business-1 account in his name.

24. Through the above scheme, the threat actor stole the logon credentials of approximately twelve Financial Institution-1 employees. Financial Institution-1 quickly revoked access to nine of those accounts. However, three of the compromised accounts were used to access sensitive Financial Insitution-1 data. On or about October 27, 2023, the threat actor then exfiltrated, or stole, that sensitive data from Financial Institution-1.

25. During the intrusion, Financial Institution-1 identified web addresses within its network logs that led to a real-time text editor (the

"Notepad") that the threat actor used to record information about the intrusion. A review of the Notepad revealed that the threat actors listed the email address evelinwang830612@gmail.com (Email Account-1). According to Google records, Email Account-1 was accessed from IP address 198.54.133.113 (the "113 IP Address") on October 27, 2023 at 21:49:24 UTC. According to Video Gaming Company-1 records, the 113 IP Address was also used to access the Remi Video Gaming Account on the same day – October 27, 2023 – at 15:50:46 UTC. Accordingly, there is probable cause to believe that OGLETREE had access to, and did access, Email Account-1.

26. The Notepad further listed a Splashtop web address (the ("Splashtop Address"). The webpage located at the Splashtop Address provides that the "team owner", or account holder, is "mqv87imj@end.tw" (the "MQV Account"). According to Splashtop records, the MQV Account was created on October 27, 2023, which is also the approximate date the intrusion into Financial Company-1 began. Splashtop records further indicate that the 163 IP Address connected to the MQV Account on October 28, 2023, at 16:36 UTC. According to Video Gaming Company-1 records, the 163 IP Address was also used to access the Remi Video Gaming Account on October 28, 2023, from 15:52 UTC to 22:25 UTC. The 163 IP Address, therefore, was used to access both the Splashtop MQV Account used in furtherance of the Financial Company-1 intrusion and the Remi Video Gaming Account at the same time. Records from the Splashtop MQV Account and the Remi Video Gaming Account also include the following additional IP address overlap:

IP Address	Splashtop MQV Account	Remi Video Gaming Account
198.44.128.209	11/01/23 18:12 UTC for a duration of 45:57	11/01/23 - 17:51:43 UTC (no logoff time noted)
43.225.189.145	10/28/23 2:08 UTC for a duration of 1:03	10/28/23 - 1:57:09 to 3:06:43
146.70.116.113	10/28/23 0:55 UTC for a duration of 1:01:44	10/28/24 - 0:47:08 UTC (no logoff time noted)

27. The Notepad also contained numerous Financial Company-1 employee names, titles, email addresses, and phone numbers as well as internal group email addresses for groups of individuals at Financial Company-1. This confidential data was stolen from Financial Company-1 during the intrusion. An accomplice later advertised other data stolen from Financial Institution-1 for sale on the dark web. The data was advertised to include the personal information, including account balances, names, dates of birth, and phone numbers of thousands of Financial Institution-1 employees.

28. A review of the OGLETREE iCloud Account revealed that on October 22, 2023 – approximately a week prior to the intrusion – OGLETREE received a phishing text on his personal phone stating, "[Financial Institution-1] Your employee schedule has been modified. [Financial Institution-1]sso.com for more information." OGLETREE was not an employee of Financial Institution-1 at the time. Like OGLETREE's receipt of a phishing text associated with Telecom Business-1, OGLETREE's receipt of this text is evidence of OGLETREE testing phishing messages prior to sending them.

Cyber Intrusion 3

29. Telecom Business-2 reported to the FBI that in or around January 2024, a network intrusion resulted in the compromise of certain Telecom Business-2 accounts.

30. Among other things, in or around January 2024, a U.S.-based Telecom Business-2 employee ("Employee-2") received numerous telephone calls from a telephone number Employee-2 did not recognize. Upon answering the last call, Employee-2 heard an automated female voice explaining that: (a) Employee-2's online account, which Employee-2 believed to be with Telecom Business-2, had been compromised; and (b) Employee-2 had to enter a code to regain access to Employee-2's account. Employee-2 further stated that the nature of the call caused Employee-2 to believe the call was legitimate. Employee-2 therefore provided the code (which Employee-2 received in a text message) through his/her telephone. Shortly after providing the code, Employee-2 became suspicious of the call. Employee-2 then notified his/her manager at Telecom Business-2. In addition, Employee-2 logged into his/her Telecom Business-2 account and identified certain new account activity from unrecognized IP addresses.

31. Based on information provided by Telecom Business-2, after Employee-2 provided the code, the threat actor then used Employee-2's credentials to further the intrusion, including by posing as Employee-2 and contacting another Telecom Business-2 employee. Through these and other acts, the threat actor accessed Telecom Business-2's network, took control over Employee-2's user account, performed recognizance on Telecom Business-2's network, and stole confidential business information from Telecom Buniness-2's network.

32. As described in more detail below, the FBI seized OGLETREE's iPhone (the "OGLTREE iPhone") pursuant to a search warrant on February 23, 2024. A search of the OGLETREE iPhone revealed that it contained Employee-2's company credentials in an application that stores passwords and account information. The "Date Created" and "Date Modified" for Employee-2's

credentials on OGLETREE's phone were listed as January 29, 2024, at 10:53pm UTC – consistent with the timing of the Telecom Business-2 intrusion.

33. According to Telecom Business-2, in or around May 2024, Telecom Business-2 suffered another intrusion into its computer network. Based on (a) information obtained by Telecom Business-2 during the January intrusion; (b) the methods used by the threat actor(s) during the May 2024 intrusion; and (c) the data stolen during the May intrusion, Telecom Business-2 believes that the confidential Telecom Business-2 data accessed and stolen during the initial January 2024 intrusion was used to illegally access Telecom Business-2's network in May 2024.

34. During the May 2024 intrusion, Telecom's Business-2's network platform was used to send more than 140,000 phishing messages in furtherance of a financial fraud scheme, including the theft of cryptocurrency. Records provided by Telecom Business-2 demonstrate that: (a) the threat actor sent test phishing messages from a compromised Telecom Business-2 account prior to sending the more than 140,000 phishing messages; and (b) two of the test messages were sent to the 7923 Phone Number (OGLETREE's phone number).

FBI Search and Seizure

35. On February 23, 2024, the FBI conducted a search of OGLETREE's residence in Fort Worth, Texas ("the Fort Worth Residence") pursuant to a court-authorized search warrant. As explained above, during the search, the FBI seized the OGLETREE iPhone. A search of the OGLETREE iPhone – in addition to the evidence described above – further revealed photos of OGLETREE as well as evidence of criminal conduct, including: (a) a screenshot of a phishing text impersonating a technology company; and (b) a screenshot of a credential harvesting phishing page impersonating a personal information manager software system. The OGLETREE iPhone also contained screenshots of cryptocurrency accounts showing tens of thousands of dollars in cryptocurrency.

OGLETREE Interview

36. During the search of OGLETREE's residence, OGLETREE was interviewed by the FBI. During this interview, OGLETREE demonstrated a knowledge of cybercrime and cybercrime techniques. OGLETREE told the FBI, "I talk to a large variety of people on [the] internet . . . I know people who commit all sorts of crimes." OGLETREE then specifically provided information on the hacking group known as "Scattered Spider." OGLETREE explained, "I know key Scattered Spider members." OGLETREE further explained, "any company getting ransom . . . that's not crypto-related, it's gonna be them . . . they target BPOs . . . because outsourcing companies they have less security." He further

explained that Scattered Spider has hacked at least five of the top "BPO" companies. Business Process Outsourcing (BPO) is a subset of outsourcing that involves the contracting of the operations and responsibilities of a specific business process to a second-party service provider. Based on my training and experience, BPOs have lower cyber security than the companies they work for, which makes intrusion into their networks easier.

37. OGLETREE further told the FBI, "I share a common interest [in] . . . finding vulnerabilities in companies . . . I've always been big with API vulnerabilities . . . When I was like 13 . . . I hacked a website . . . there was this Chinese gambling site . . . I was able to hack the crashed API . . . I was able to make like 0.5 [in cryptocurrency]. . . it was like 20K." OGLETREE further detailed, "when I was 12, and was around these SIM swappers, I started simming . . . when I was 13 and I got arrested like 6 months later." "Simming" is another name for "SIM swapping," which is a technique used to gain control of a phone number. With that control, cyber criminals can take advantage of two-factor authentication to gain access to bank, cryptocurrency, social media, and other accounts.

Cryptocurrency Laundering

38. Two days after the FBI searched OGLETREE's residence, a Telegram user ("User-1") later identified as OGLETREE contacted the provider of a cash for cryptocurrency money laundering service (the "Cash Service"). On February 25, 2024, OGLETREE stated, "I need $50k cash." OGLETREE then increased his request to "$75k" and asked that the cash be sent in OGLETREE's father's name to the Fort Worth Residence. At the time, OGLETREE was apparently unaware that the Cash Service was part of an undercover FBI operation. The Cash Service provided a wallet address to which OGLETREE was to send cryptocurrency for the exchange. A review of blockchain evidence indicates that on February 25, 2024, 668.78 XMR was sent to the wallet provided. XMR is the abbreviation for Monero. According to its website, Monero is the only major cryptocurrency where every user is anonymous by default. With Monero, the sender, receiver, and amount of every transaction are hidden. The Cash Service provided a USPS tracking number and mailed $75,000 (the value of any cryptocurrency OGLETREE sent minus a fee) to OGLETREE's Fort Worth Residence. The tracking information indicates that the package was delivered on February 29, 2024, to OGLETREE's Fort Worth Residence. On February 29, 2024, OGLETREE confirmed, "I got the money," noting "the USPS driver forged a signature on the package and left it in the mailbox because he was too lazy to come to the door."

39. A Telegram user believed to be OGLETREE also used the Cash Service to convert cryptocurrency to cash on multiple earlier occasions, including three times in 2023.

40. For example, in May 2023, Telegram communications between the Cash Service and OGLETREE using another display name, "X," indicate that OGLETREE twice traded large amounts of cryptocurrency for cash that month. On May 19, 2023, Telegram display name "X" asked the Cash Service, "How much for $20k cash USD?" The Cash Service asked if "X" had "traded in past." "X" responded, "Yes on old telegrams, I forgot usernames. Have done about $80k through you." "X" noted, "I already cleaned this money. BTC > XMR Via Non-KYC exchanges > ETH on another Non-KYC exchange." "Non-KYC" or "no Know Your Customer," refers to a service or exchange that does not require personal information to verify a customer's identity. ETH is the abbreviation for ether, the native cryptocurrency of the Ethereum platform. In my training and experience, the use of Monero, non-KYC exchanges, and multiple blockchains are used to obfuscate the source and movement of cryptocurrency.

41. "X" further stated, "$23k for 20k sounds fair," indicating he wanted to pay $3,000 in fees to convert $20,000 worth of cryptocurrency to cash. The Cash Service initially negotiated a higher fee, for a total of "23.7" but then negotiated up to "24.1" because "X" wanted to send USDT, a different type of cryptocurrency. USDT, also known as Tether, is a cryptocurrency stablecoin that's pegged to the US dollar at a 1:1 ratio. This means that one USDT is theoretically always worth one USD. The Cash Service provided a cryptocurrency wallet address to "X." A review of blockchain evidence indicates that on May 19, 2023, 24100 USDT, worth $24,100 was sent to the wallet provided. The Cash Service thereafter shipped a package of cash via USPS on May 19, 2023, to a recipient "Steven Ellis" and an address in Granbury, Texas ("Granbury Address-1") provided by "X." Granbury Address-1 matches the address that is on OGLETREE's Texas identification card. Ellis is the last name of OGLETREE's father.

42. On May 20, 2023, "X" told the Cash Service that he needed "the Delivery name changed" and that he would "pay $1000 for this" because "photo ID" would be required "to get packages." "X" clarified that he previously "gave [a] fake name" but would now "give my mules name." "X" then provided the name of OGLETREE's father. "X" agreed to pay $6,000 so the Cash Service would have a USPS employee help retrieve the previously delivered package and change the recipient's name. A review of blockchain evidence indicates that on May 20, 2023, 6000 USDT, worth $6000, was sent. Thereafter, the Cash Service provided an updated tracking number. USPS tracking data reflects that the package was delivered on May 22, 2023, to OGLETREE's address in Granbury, TX.

43. On May 25, 2023, "X" again reached out to the Cash Service on the same Telegram message thread and asked, "how much for $25k cash." "X" and the Cash Service agreed "30k for 25k," meaning "X" would pay a $5,000 fee for the Cash Service to convert $25,000 worth of cryptocurrency to cash. "X" provided a new shipping recipient and address, noting it was a "mule house." Specifically, "X" directed that the cash be sent to "Steven Durango" at an address in Granbury, Texas ("Granbury Address-2"). A relative of OGLETREE reported to the FBI that s/he resided at this address in 2022. Tax records indicate that Granbury Address-2 had the same owners in 2022 through 2024. Further, Apple indicate that "Steven Durango" is the same name that was used to register OGLETREE's Apple iCloud account. A review of public records indicates that no individual by the name of "Steven Durango" resided in Granbury, Texas at the time, indicating that the name was false. Thereafter, the Cash Service provided a tracking number. The Cash Service also provided a cryptocurrency wallet address to "X." A review of blockchain evidence indicates that on May 25, 2023, 30000 USDT, worth $30,000 was sent to the wallet provided. USPS tracking data reflects that a package was delivered on May 26, 2023, to the Granbury Address-2.

44. On October 12, 2023, "X" again contacted the Cash Service and asked, "How much do you charge if I want $20k in cash?" "X" and the Cash Service ultimately agreed the Cash Service would convert $30,000 worth of cryptocurrency to cash for a $3,000 fee. The Cash Service provided a cryptocurrency wallet address, and blockchain data reflects that on October 13, 2023, 1.23558479 BTC worth $33,041 was sent to the Cash Service on October 12, 2023. "X" asked that the cash be sent to a specific address in Miami, Florida (the "Miami Address") with OGLETREE's father listed as the recipient. Airbnb records indicate that the residence located at the Miami Address was rented through Airbnb using an account in the name of OGLETREE's father. The rental was for three guests, began on September 24, 2023, and was for 30 nights (or until on or about October 24, 2023). The Cash Service provided a tracking number. USPS tracking data reflects that the package was delivered on October 18, 2023, to the Miami Address.

45. OGLETREE's iCloud account contains a screen shot dated November 27, 2023 – approximately one month following the above transfer – of a photo taken on a messaging application of a person's hand holding a stack of cash:

The formatting of the photo matches other screen shots on OGLETREE's iCloud of the same messaging application that OGLETREE took, including photos of himself, indicating that OGLETREE took the photo of the cash.

46. During the October 2023 transaction, "X" and the Cash Service discussed cryptocurrency theft. "X" stated he makes money from "crypto theft" and earned "$300k past 24 hours." He further explained, "in this instance there was an exploit on [Cryptocurrency Company-3] to bypass SMS 2FA . . . It got patched today." "X" noted, "you can make $10m a year easily doing it if dedicated." "X" then provided a summary of how to steal cryptocurrency, including a suggestion that the Cash Service "hack internet service provider with lots of customer emails" and direct cryptocurrency customers to a "phishing site to phish 2fa and withdraw" the cryptocurrency. "2fa" stands for two-factor authentication, a data security feature that requires two forms of identification to access resources and data.

47. Based upon the evidence in this case and my training and experience, the true identity of Telegram users "User-1" and "X" is OGLETREE. First, "User-1" and "X" directed that the packages of cash be mailed to addresses where OGLETREE was staying at the time, or an address of OGLETREE's relative. Second, the users had the packages of cash sent to OGLETREE's father or a name OGLETREE used to register his Apple account. Further, OGLETREE made money through cryptocurrency theft, as described by "X" to the Cash Service.