

FILED
Jul 23 2020
SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT
for the
Northern District of California

United States of America)
v.)
MASON JOHN SHEPPARD)
)
)
)
)
)

Case No. 20-mj-70996 MAG

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of July 15, 2020 in the county of San Francisco in the
Northern District of California, the defendant(s) violated:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. Sections 1349, 1030, 1956(h)	Conspiracy to Commit Wire Fraud, Computer Intrusion, Money Laundering (See Attached Penalty Sheet)

This criminal complaint is based on these facts:

See Attached Affidavit of IRS-CI Special Agent Tigran Gambaryan

Continued on the attached sheet.

/s/ Tigran Gambaryan via telephone

Approved as to Form:
_____/s/_____
AUSA Dawson

Complainant's signature
Tigran Gambaryan, IRS-CI Special Agent

Printed name and title

Sworn to before me by telephone.

Date: 7/22/2020



Judge's signature

City and state: San Francisco, CA

Hon. U.S. Magistrate Judge Alex G. Tse

Printed name and title

Penalty Sheet

18 U.S.C. § 1030(a)(2)(C) (computer intrusion)

- 5 years' imprisonment
- \$250,000 fine
- 3 years' supervised release
- \$100 special assessment
- Restitution
- Forfeiture

18 U.S.C. § 1349 (wire fraud conspiracy)

- 20 years' imprisonment
- \$250,000 fine
- 3 years' supervised release
- \$100 special assessment
- Restitution
- Forfeiture

18 U.S.C. § 1956(h) (money laundering conspiracy)

- 20 years' imprisonment
- \$250,000 fine
- 3 years' supervised release
- \$100 special assessment
- Restitution
- Forfeiture

UNITED STATES DISTRICT COURT)

)

NORTHERN DISTRICT OF CALIFORNIA)

AFFIDAVIT

I. INTRODUCTION AND AGENT BACKGROUND

I, Tigran Gambaryan, being duly sworn, state as follows:

1. I am employed as a Special Agent with the Internal Revenue Service Criminal Investigation (“IRS-CI”) in Washington, D.C. and have been so employed since 2011. I completed the required Special Agent training at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia. This training included eleven weeks of criminal investigative training, including courses in law enforcement techniques, federal criminal statutes, conducting criminal investigations, and the execution of search warrants. This training also included instruction in the law of search and seizure under the Fourth Amendment of the United States. In addition to the criminal investigative training, I completed a Special Agent Basic Training course lasting thirteen and one-half weeks, which included courses in financial investigative techniques, legal principles, and statutes representing criminal violations of the United States Code as enumerated in Titles 18, 26, and 31. I have been involved in numerous investigations of alleged violations of the Internal Revenue Code, money laundering statutes, wire fraud, and related offenses. I have participated in numerous interviews of witnesses and have been the affiant of federal search warrants involving suspected criminal violations where records, of the type involved in this investigation, were seized. Prior to my IRS-CI employment, I was as an auditor for California’s Franchise Tax Board, where I investigated abusive tax shelters.

2. I am currently assigned to IRS-CI Cyber Crimes Unit (“CCU”) in Washington, D.C. I have been assigned to the CCU for more than three years. I have developed a specialty in cyber and digital currency crimes. I have been assigned to numerous cases while at the CCU, including cases involving bitcoin and other cryptocurrencies. For example, in 2014, I was assigned to investigate former U.S. Drug Enforcement Administration Agent Carl Force and former U.S. Secret Service Agent Shaun Bridges who were members of the Baltimore Silk Road Task Force. The investigation into Force and Bridges was the first known U.S. investigation that relied on bitcoin clustering and blockchain tracing to identify bitcoin money laundering, and led to their convictions and the recovery of more than \$12 million in bitcoin. Since that investigation, I have successfully used bitcoin clustering tools and bitcoin blockchain tracing during several multi-billion dollar criminal investigations. I have also taught bitcoin clustering and tracing to law enforcement in the United States and abroad, including to law enforcement in Tokyo, at Interpol, and at Europol. I also co-developed a bitcoin clustering and tracing curriculum that is used to train all IRS-CI special agents at FLETC.

3. This affidavit is made in support of an issuance of an arrest warrant and a criminal complaint alleging that **Mason John Sheppard**, also known as “**Chaewon**” and “**ever so anxious#001**”:

- Aided and abetted intentional access of a protected computer and obtaining information, in violation of Title 18, United States Code, Section 1030(a)(2)(C) (Count One);
- Conspired with others to commit a violation of Title 18, United States Code, Section 1343 (wire fraud), in violation of Title 18, United States Code, Section 1349 (Count Two); and
- Conspired with others to commit money laundering, in violation of Title 18, United States Code, Section 1956(h) (Count Three).

4. The facts set forth in this affidavit are based on information that I have obtained from my personal involvement in the investigation and from other law enforcement officers who have been involved in this investigation (including special agents of the Federal Bureau of Investigation and United States Secret Service).

II. DEFINITIONS

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

6. **Server**: A server is a computer that provides services to other computers. Examples include web servers which provide content to web browsers and email servers which act as a post office to send and receive email messages.

7. **Domain**: “Domain” is short for “domain name.” Under 18 U.S.C. § 3559(g)(2)(B), the definition of “domain name” is based on the Trademark Act, under 15 U.S.C. § 1127. Under the Trademark Act, “domain name” means “any alphanumeric designation which is registered with or assigned by any domain name registrar, domain name registry, or other domain name registration authority as part of an electronic address on the Internet.” A “subdomain” was a subdivision of a domain.”

8. **Domain Name System**: The Domain Name System (“DNS”) is a hierarchical and decentralized Internet service that translated domain names into Internet Protocol (“IP”) addresses. A “top-level domain” is the last segment (i.e., suffix) in a domain (e.g., “.com” or “.net”) associated with the highest level of the DNS.

9. **Registrar & Registrant**: “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 managed top-level domains, known as registries. The domain name registrant is bound by the

terms and conditions of the registrar with which it registered its domain name, for instance adhering to a certain code of conduct or indemnifying the registrar and registry against any legal or civil action taken as a result of use of the domain name.

10. **Bitcoin**: Bitcoin is a type of virtual currency, circulated over the Internet as a form of value. Bitcoin was not issued by any government, bank, or company, but rather were generated and controlled through computer software operating via a decentralized, peer-to-peer network. Bitcoin is just one of many varieties of virtual currency.

11. **Bitcoin exchangers**: Exchangers are persons or entities in the business of exchanging fiat currency (currency that derives its value from government regulation or law, such as the U.S. dollar) for bitcoin, and exchanging bitcoin for fiat currency. When a user wishes to purchase bitcoin from an exchanger, the user will typically send payment in the form of fiat or other convertible virtual currency to an exchanger, usually via wire or ACH, for the corresponding number of bitcoin based on a fluctuating exchange rate. The exchanger, often for a commission, will then typically attempt to broker the purchase with another user of the exchange that is trying to sell bitcoin, or, in some instances, will act as the seller itself. If the exchanger can place a buyer with a seller, then the transaction can be completed. Based on my training and experience, bitcoin exchanges send confirmation emails to the email account used to register the member exchange account for each deposit, trade, and/or withdraw bitcoin and fiat transactions conducted by the user on the exchange.

12. **Bitcoin address**: Bitcoin addresses are the particular virtual locations to which bitcoin are sent and received. A Bitcoin address is analogous to a bank account number and was represented as a 26-to-35-character-long case-sensitive string of letters and numbers.

13. **Private Key**: Each bitcoin address is controlled through the use of a unique corresponding private key, a cryptographic equivalent of a password needed to access the address. Only the holder of an address's private key can authorize a transfer of Bitcoin from that address to another Bitcoin address.

14. **Bitcoin Wallet**: A bitcoin wallet is an application that holds a user's bitcoin addresses and private keys. A bitcoin wallet also allows users to send, receive, and store bitcoins. It is usually associated with a bitcoin address.

15. **Blockchain**: All bitcoin transactions are recorded on what is known as the blockchain. The blockchain is essentially a distributed public ledger that keeps track of all bitcoin transactions, incoming and outgoing, and updates approximately six times per hour. The blockchain records every bitcoin address that has ever received bitcoin and maintains records of every transaction and all the known balances for each bitcoin address. As a result, forensic analytical tools are able to review the blockchain, identify which bitcoin addresses are related and owned by the same individual or entity (called a cluster), and calculate the total number of bitcoins in all of these related bitcoin addresses.

16. **Cluster**: A cluster is a collection of bitcoin addresses that can be attributed to one person or entity through various means, including co-spending, in order to determine the number of bitcoin held by an individual. In other words, a cluster is an estimate of all of the bitcoin addresses (and its bitcoins) contained in a user's bitcoin wallet or wallets. Because the blockchain records every bitcoin address, and maintains records of every transaction, and all the known balances for each bitcoin address, forensic computer experts are able to create clustering algorithms that examine the entire history of bitcoin transactions recorded on the blockchain and make logical connections between different bitcoin addresses.

III. FACTS ESTABLISHING PROBABLE CAUSE IN SUPPORT OF THE ARREST WARRANT AND CRIMINAL COMPLAINT

A. BACKGROUND

13. Twitter, Inc. ("Twitter") operates a microblogging and social networking service utilized by various high-profile individuals, including politicians, celebrities, and musicians such as Bill Gates, Elon Musk, Kanye West, Joe Biden, Barack Obama, and U.S. President Donald

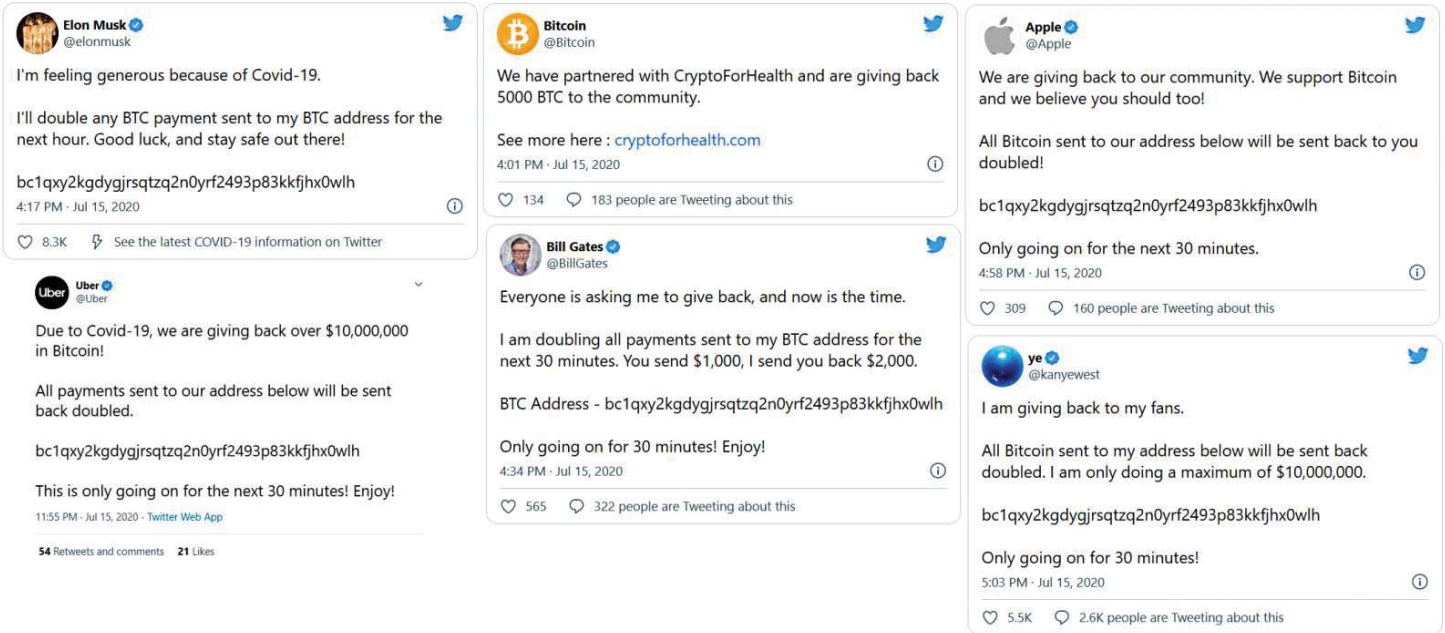
Trump. Many such high-profile individuals have “verified” their accounts by proving to Twitter they are indeed the real person named on the account.

14. Per statements made by Twitter, numerous media reports, public victim statements, and through this investigation, on July 15, 2020, multiple high-profile verified accounts were compromised, including accounts belonging to Bill Gates, Elon Musk, Kanye West, Joe Biden, Barack Obama, Jeff Bezos, Mike Bloomberg, Warren Buffett, Benjamin Netanyahu, and Kim Kardashian. Accounts belonging to cryptocurrency exchanges, such as Binance, Gemini, Coinbase, Bitfinex, and AngeloBTC were also compromised, as were prominent companies like Apple Inc. (“Apple”) and Uber Technologies Inc. (“Uber”). Per a statement made by Twitter on July 16, 2020, via Twitter’s communications account @TwitterSupport, approximately 130 Twitter user accounts were affected in the hack: “Based on what we know right now, we believe approximately 130 accounts were targeted by the attackers in some way as part of the incident. For a small subset of these accounts, the attackers were able to gain control of the accounts and then send Tweets from those accounts.”

15. According to numerous media reports, and Twitter’s own statements, the malicious actor(s) gained access to the Twitter accounts by compromising a Twitter employee’s account. In a statement made by Twitter on July 15, 2020, via @TwitterSupport, Twitter stated, “We detected what we believe to be a coordinated social engineering attack by people who successfully targeted some of our employees with access to internal systems and tools.”

16. The actor(s) then used their access to the compromised Twitter accounts to post messages directing victims to send cryptocurrency to accounts, including, and especially, the bitcoin address “bc1qxy2kgdygjrqtzq2n0yrf2493p83kkfjhx0wlh” (hereinafter, “the bc1qxy address”). On some of the Twitter posts, the actor(s) provided the actual bitcoin address, while on others the posts guided victims to a website hosted at the domain cryptoforhealth.com, which also provided the same bitcoin address. In all cases, the Twitter postings said that individuals who sent any bitcoin to the aforementioned address would receive double the bitcoin in return.

17. Below are screen captures of some of these Twitter posts from the compromised accounts belonging to Elon Musk, Bitcoin, Apple Kanye West, Bill Gates, and Uber:¹



18. Apple confirmed to the FBI on July 16, 2020 that it did not post the message above. Numerous other victims—including Bill Gates—made public statements that their Twitter accounts had also been hacked, and that they did not write or post the messages directing individuals to send them bitcoin.

¹ See Sergiu Gatlan, *Scammers hacked Twitter and hijacked accounts using admin tools*, BLEEPINGCOMPUTER (Jul. 16, 2020, 10:20 AM), <https://www.bleepingcomputer.com/news/security/scammers-hacked-twitter-and-hijacked-accounts-using-admin-tool/>.

19. Twitter messages were posted on July 15, 2020 to Twitter accounts belonging to cryptocurrency exchanges Kucoin, Coinbase, Gemini, and Binance, which directed users to follow the link for a website hosted at the domain cryptoforhealth.com.²

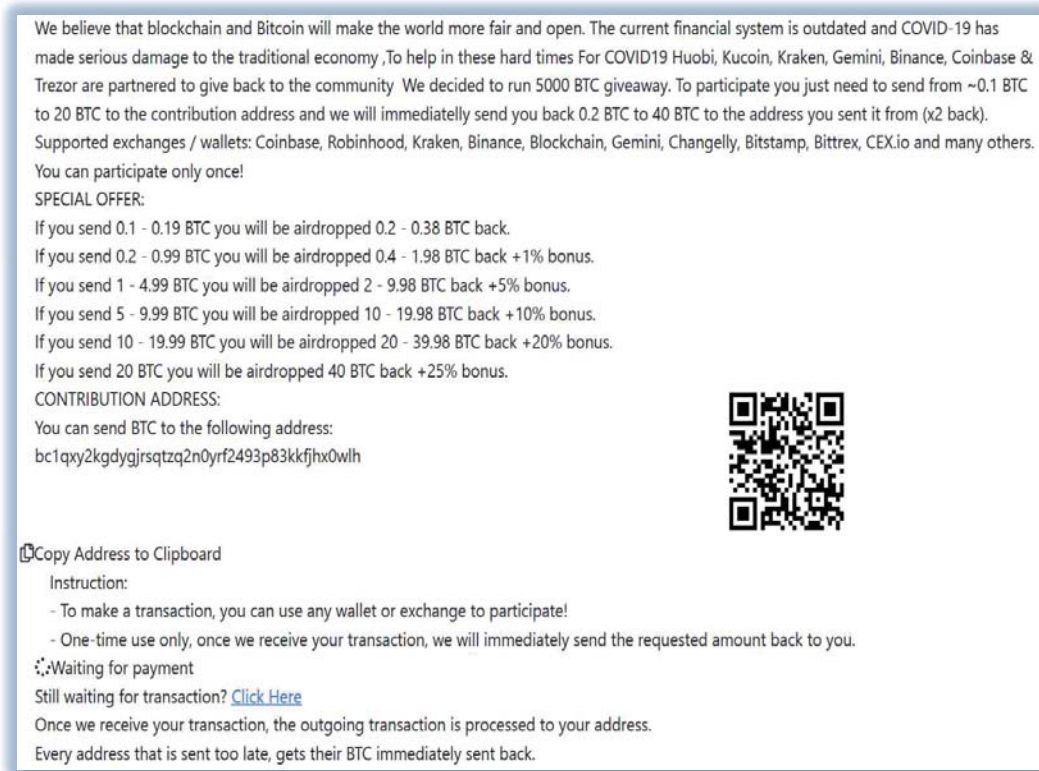


20. Coinbase confirmed to the FBI and IRS-CI on July 16, 2020, that it did not post the message above.

21. The website hosted at cryptoforhealth.com led to a webpage that, like the other Twitter posts, directed individuals to send bitcoin to the the *0wlh address, in exchange for twice the amount of bitcoin deposited in return.

² See Danny Nelson, *Twitter Hack Takes Down Joe Biden, Elon Musk Accounts in Widespread Bitcoin Scam Attack*, COINDESK, <https://www.coindesk.com/hackers-take-over-prominent-crypto-twitter-accounts-in-simultaneous-attack> (last visited Jul. 17, 2020, 4:08 PM).

22. Though the cryptoforhealth.com website had been taken down as of July 16, 2020, the below image from the website was taken from an archive of the site on the “Wayback Machine”³:



23. As described below, the actor(s)’ fraud campaign was successful, as the bitcoin account received hundreds of incoming transfers of bitcoin. No bitcoin was ever returned, much less doubled.

24. I believe that the actors(s) who controlled the cryptoforhealth.com domain, and the *0wlh address address, hacked popular, and trusted, verified Twitter accounts for high-profile individuals and companies – including those belonging to cryptocurrency exchanges. I further believe that the same actor(s) used those trusted, now hacked, accounts to post messages, reaching those Twitter accounts’ followers, with an offer to double their bitcoin—both directly, and via a

³ Archive of cryptoforhealth.com on July 15, 2020, WAYBACK MACHINE, https://web.archive.org/web/*/cryptoforhealth.com (last visited Jul. 16, 2020).

message posted on the website hosted at the domain cryptoforhealth.com—in order to entice individuals into sending bitcoin to the *0wlh address. The individual(s) then stole the bitcoin and transferred it out of the account.

B. AFTER THE TWITTER HACK, THERE WERE APPROXIMATELY 415 TRANSFERS INTO THE SUSPECT BITCOIN ADDRESS, WORTH \$117,457.58

25. Between July 15, 2020, when the hack of the verified Twitter accounts occurred, and July 16, 2020, the bitcoin wallet associated with the *0wlh address had sent or received 426 transfers. Approximately 415 of those transfers consisted of transfers from other bitcoin addresses into the *0wlh account, totaling approximately 12.86 bitcoin, worth approximately \$117,457.58 as of July 16, 2020 (at a rate of \$9,133.56 per bitcoin). Eleven (11) of those transfers were from the wallet associated with the *0wlh address to other bitcoin addresses, siphoning off 99.74% of the bitcoin deposited, or 12.83 bitcoin, worth \$117,183.57, leaving a remaining balance of \$274.01 in the account. No bitcoin was returned to the victims.

26. In my training and experience, individuals will shuffle bitcoin from one wallet to another in order to obfuscate its origin. Based on my training and experience, I believe the above-described transfers out of the origin bitcoin wallet to other addresses were intended to conceal the origin of the funds, in violation of 18 U.S.C. §§ 1956 and 1957 (money laundering and money laundering conspiracy).

C. KIRK#5270'S INVOLVEMENT IN THE TWITTER HACK

27. I have probable cause to believe that an unknown individual, identified by the online moniker of “Kirk#5270,” played a central role in the compromise of Twitter on July 15, 2020. Pursuant to a search warrant signed by U.S. Magistrate Judge Sallie Kim in the Northern District of California on July 17, 2020, Discord, Inc.⁴ provided content, which included Discord

⁴ Discord is a free voice over internet protocol (“VoIP”) application and digital distribution platform. It was initially designed for the video gaming community but has since expanded to a wider audience. Discord offers chat channels where users can communicate via text messages, voice, and video.

chats between an individual utilizing the username “Kirk#5270” and others, in which “Kirk#5270” said that he/she could reset, swap, and control any Twitter account at will, and would do so in exchange for bitcoin transfers.

28. Among the content provided by Discord was an image sent by “Kirk#5270” to an unidentified individual who used the Discord moniker “Rolex#0373” of an internal administrative tool used by Twitter to make changes to user accounts. Upon receiving the image, “Rolex#0373” responded with “Damn”, and later, “I’m in.” “Kirk#5270” immediately responded by providing a Bitcoin address, “1Ai52Uw6usjhpcDrwSmkUvjuqLpcznUuyF” (hereinafter, the “Kirk#5270 address”). Based on my training and experience, I understand this to be a Bitcoin address used to send and receive bitcoin payments and that “Kirk#5270” was requesting payment via bitcoin for access to Twitter accounts.

29. I have reviewed chats between “Kirk#5270” and several other users, which point to “Kirk#5270” being involved in the Twitter compromise. In one Discord chat on July 15, 2020, “Kirk#5270” stated, “I work for Twitter” and “I can claim any name, let me know if you’re trying to work.” In another chat from the same day between “Kirk#5270” and Discord user “Rolex#0373”, “Kirk#5270” stated, “I work for Twitter. I can claim any @ for you.”⁵

30. In a separate Discord chat with the user associated with moniker “**ever so anxious#001**” on July 15, 2020, “Kirk#5270” continued to provide proof of access to a wide variety of Twitter accounts by providing images of Twitter’s internal administrative tool for accessing those accounts. For example, “Kirk#5270” provided images of administrator-level access to Twitter accounts “@bumblebee,” “@sc,” “@vague,” and “@R9,” among many others. Based on the chat as a whole, it appears that “**ever so anxious#001**” began to find buyers for Twitter usernames. For instance, “ever so anxious#001” writes, “I have a buyer rn,” “someone’s interested,” and “i have a buyer for 50 for 3k u down?” Among the discussions, the user associated

⁵ Based on my understanding of various social media platforms, the symbol “@” immediately precedes a username. The reference to “claim any @ for you” is generally a reference to having access to any social media username.

with moniker “ever so anxious#001” wrote, “send your bitcoin addy too,” to which “Kirk#5270” provided the “Kirk#5270” address. “Kirk#5270” mentioned the “Kirk#5270” address approximately sixteen times throughout the chat in discussions about payment for accounts. Additionally, “Kirk#5270” asked “ever so anxious#001” “What’s ur ugu”?⁶ The user “ever so anxious#001” responded, “chaewon.” Portions of this chat are excerpted below:

Date and Time	Message Sender	Message
2020-07-15 12:26:40.175000+00:00	Kirk#5270	1Ai52Uw6usjhpcDrwSmkUvjuqLp cznUuyF
2020-07-15 12:25:45.024000+00:00	ever so anxious#0001	send ur btc addyy too
2020-07-15 13:23:22.043000+00:00	Kirk#5270	1Ai52Uw6usjhpcDrwSmkUvjuqLp cznUuyF
2020-07-15 13:23:13.879000+00:00	ever so anxious#0001	send addyy
2020-07-15 14:00:56.066000+00:00	Kirk#5270	5k for all 3?
2020-07-15 13:59:50.215000+00:00	ever so anxious#0001	also is @vampire doable
2020-07-15 13:59:05.494000+00:00	ever so anxious#0001	guy wants them
2020-07-15 13:59:03.181000+00:00	ever so anxious#0001	5k for @xx 3k @dark let me know

31. Per information provided to the FBI by Twitter, the accounts of @xx, @dark, and @vampire mentioned in the chat excerpted above were compromised on July 15, 2020.

32. The *New York Times* also reported that an individual referred to as “Kirk” played a central role in the Twitter compromise.⁷ The *New York Times* received screenshots of conversations involving Kirk stating, “i work at twitter / don’t show this to anyone / seriously.” This followed with Kirk’s demonstration of his/her ability to take control of valuable Twitter accounts. The *New York Times* identified the individual in contact with Kirk as using the Discord moniker “lol”. As discussed below, parts of the *New York Times* article have been confirmed by the FBI.

⁶ The mention of “ugu” by “Kirk#5270” is believed to be a request for the username of “ever so anxious#001” on the OGUUsers forum, as further detailed below, an online forum popular among people involved in the hijacking of online accounts.

⁷ See Nathaniel Popper and Kate Conger, *Hackers Tell the Story of the Twitter Attack From the Inside*, N.Y. TIMES (Jul. 17, 2020), <https://www.nytimes.com/2020/07/17/technology/twitter-hackers-interview.html>.

D. PROBABLE CAUSE LINKING “CHAEWON” AND “EVER SO ANXIOUS#0001” ACCOUNTS WITH MASON JOHN SHEPPARD

33. On July 15, 2020, the day of the compromise of Twitter accounts, users on the forum OGUUsers.com (“OGUsers”) began advertising the sale of illicit access to any Twitter account. Based on my training and experience, the OGUUsers forum is abused by criminal networks. In one such public post entitled “Pulling email for any Twitter/Taking Requests,” a user named “**Chaewon**” advertised that he could change email addresses tied to any Twitter account for \$250 and provide direct access to accounts for between \$2,500 and \$3,000. In this post, “**Chaewon**” stated the following:

Price: 250

you heard me, 250\$ per email to any twit acc

will sell multiple for less ie 2 for 420 3 for 675

btc only

u go first or @lol can hold funds idc

taking requests 2.5k – 3k per @

usernames claimed done so far:

anx**s

dr*g

**

**

ob*nna

d**k

*

*

people who have used this service: @maxwell @jawad

ever so anxious#0001 – dont message saying hey say the twit youre interested in

This is NOT a method, you will be given a full refund if for any reason you aren't given the email/@, however if it is reversed/suspended I will not be held accountable.

34. Based on my training and experience, I believe this OGUsers advertisement publicly advertised the sale of stolen Twitter accounts and referred interested buyers to contact **“ever so anxious#0001”** on the Discord platform.

35. The seized Discord records described in paragraph 27 above included chat communications between multiple individuals involved in the events that led up to the aforementioned compromise of Twitter servers and the sale of Twitter accounts via bitcoin payments.

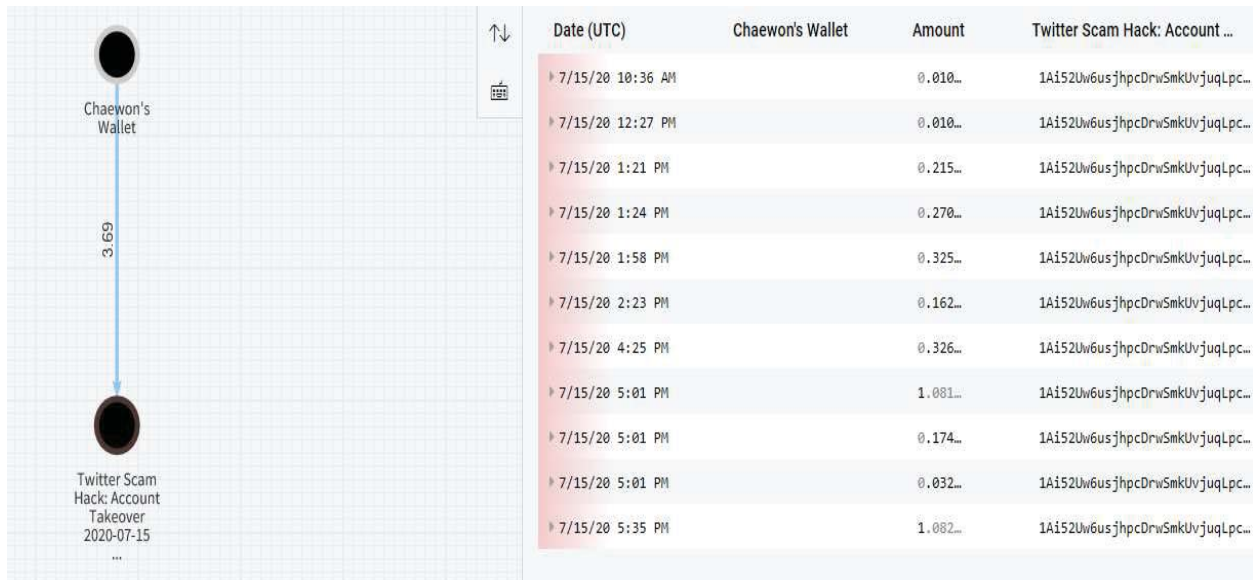
36. I reviewed the content of these chats, including a chat between Discord users **“ever so anxious#0001”** and **“Kirk#5270”**. In this chat, **“ever so anxious#0001”** purchases stolen Twitter username **@anxious** from **“Kirk#5270”** by paying bitcoin to the **Kirk#5270** address. After this initial transaction, **“ever so anxious#0001”** brokered the purchase of additional stolen Twitter usernames for his contacts and via his advertisement on the OGUsers forum. For example, on July 15, 2020, between approximately 7:16 AM ET to 2:00 PM ET, **“ever so anxious#0001”** discusses the takeover of at least fifty Twitter usernames. These usernames were not verified usernames belonging to well-known celebrities or political figures, but instead were rare and original usernames such as **@L**, **@bitch**, and **@w**. In all of these transactions, **“Kirk#5270”** provides the **Kirk#5270** address to **“ever so anxious#0001”** for payment. According to Twitter, at least ten of the transactions brokered by **“ever so anxious#0001”** resulted in Twitter usernames being stolen from their actual owners—to include **@obinna** and **@drug**.

37. In the aforementioned Discord chat, **“ever so anxious#0001”** told **“Kirk#5270”** that his OGUsers username is **“Chaewon.”** Likewise, the **Chaewon** advertisement on OGUsers forum claims that Twitter usernames **“anxi**s,” “dr*g,”** and **“ob*nna”** were already successfully taken-over by this new service, consistent with the Twitter usernames discussed in the Discord chats between **“ever so anxious#0001”** and **“Kirk#5270”**.

Blockchain Analysis

38. Using blockchain analysis, I analyzed the bitcoin deposits and withdrawals to the wallet associated with the Kirk#5270 address. I found that this wallet received several large deposits of bitcoin on July 15, 2020, totaling approximately 3.69 bitcoin (approximately \$33,000 at the time of payment) from wallet cluster bc1qdme7m3zy450m5gl0w9n2mrh8t8h6448xfzdlvv (hereinafter, “the Chaewon Cluster”). The timing and amounts of these deposits correspond with the timing of payment requests made by “Kirk#5270” to “**ever so anxious#0001**” for stolen Twitter usernames.

39. Using blockchain analysis, I analyzed the bitcoin deposits and withdrawals to the Chaewon Cluster. I found several Binance bitcoin exchange deposits and withdrawals. I found that on July 15, 2020, the pattern of payment deposited and withdrawn from the Chaewon Cluster shows that “**ever so anxious#0001**” used this bitcoin wallet cluster to broker bitcoin transfers between the buyers of various stolen Twitter usernames and “Kirk#5270”. Indeed, during the relevant time frame on July 15, 2020, “**ever so anxious#0001**” received approximately 4.48 bitcoin (approximately \$40,065 at the time of payment) in this wallet cluster and paid 3.69 bitcoin (approximately \$33,000 at the time of payment) to “Kirk#5270”:



40. I obtained transaction records from U.S.-based bitcoin exchange Coinbase related to Coinbase-controlled wallets that paid into the Chaewon Cluster. These records show that Coinbase customers made several bitcoin payments that valued \$250—which is the amount advertised by **Chaewon**—to the wallet cluster. Some of these Coinbase transactions had user notes associated with them. At least one such note stated “emails,” consistent with the **Chaewon** advertisement. Based on my analysis of Discord chats, posts **Chaewon** made on the OGusers forum, and bitcoin exchange records, I believe these \$250 payments were for the takeover of Twitter usernames.

41. In summary, based on the facts described above, as well as my training and experience, I believe that **Chaewon** acted as a broker for “Kirk#5270,” sending criminally derived proceeds from the sale of Twitter accounts to “Kirk#5270” for the exchange for compromised Twitter accounts.

Attribution of Mason John Sheppard

42. On April 2, 2020, the administrator of the OGUsers forum publicly announced that OGUsers website was successfully hacked. Shortly after the announcement, a rival criminal hacking forum publicly released a link to download the OGUsers forum database, claiming it contained all of the forum’s user information. The publicly released database has been available on various websites since approximately April 2020. On or about April 9, 2020, the FBI obtained a copy of this database. The FBI found that the database included all public forum postings, private messages between users, IP addresses, email addresses, and additional user information. Also included for each user was a list of the IP addresses that user used to log into the service along with a corresponding date and timestamp.

43. I reviewed records and communications that are part of this publicly-released database. I also found that on February 4, 2020, **Chaewon** exchanged private messages on OGUsers with another user of the forum during which **Chaewon** made a purchase of a video game

username and was instructed to send bitcoin to address 188ZsdVPv9Rkdiqn4V4V1w6FDQVkJ7pDf4 (hereinafter, “the Chaewon purchase address”).

44. Using blockchain analysis, I analyzed the bitcoin deposits and withdrawals to the Chaewon purchase address. I found that on February 5, 2020, the Chaewon purchase address received approximately .088 bitcoin from the Chaewon Cluster, the same bitcoin cluster from which on July 15, 2020, “**ever so anxious#0001**” received bitcoin and sent bitcoin to “Kirk#5270.” I also analyzed the IP addresses used to connect to the **Chaewon** account in the publicly-available OGUUsers forum database. I found that on April 29, 2017, the IP address 79.66.149.155 was used to connect to the **Chaewon** account, as well as another OGUUsers account, **Mas**. This IP address resolves to a U.K.-based Internet Service Provider called Talk Talk Communications. Based on my training and experience, I believe that the individual who controlled the **Chaewon** account also controlled the **Mas** account.

45. The **Mas** account on the OGUUsers forum is associated with the e-mail address, **masonhppy@gmail.com**, along with other email addresses. Based on my knowledge and experience, I know that users of forums such as OGUUsers may change their username and then publicly announce to the forum their previous username. On several occasions on February 11, 2020 and February 15, 2020, **Chaewon** publicly posted on OGForum, “IT IS MAS I AM MAS NOT BRY I AM MAS MAS MAS!@”

46. Based on the information gathered from the OGUUsers database, records were obtained from Coinbase for accounts linked to **masonshppy@gmail.com**. Coinbase provided the following information:

USER ATTRIBUTES ***

USER ID	599094f007e57a01cf67121d
NAME	mason sheppard

EMAIL masonshppy@gmail.com

CREATED August, 13 2017 11:05am PDT

Coinbase also provided a photo of a driver's license in the name of **Mason John Sheppard** from the United Kingdom and with an address and date of birth for **Sheppard**.

47. As stated above, the Kirk#5270 address received several large deposits of bitcoin from the Chaewon Cluster on July 15, 2020, totaling approximately 3.69 bitcoin. I analyzed the transaction history for the Chaewon Cluster and found several bitcoin exchange deposits and withdrawals associated with Binance, a virtual currency exchange.

48. I obtained records from Binance related to the Chaewon Cluster, and having reviewed the account information, I know that all of the deposits into and withdrawals from the Chaewon Cluster are directly related to two different accounts. Binance provided records related to these two accounts, which revealed that both accounts are controlled by **Mason John Sheppard**, using the email addresses masonshppy@gmail.com and chaengy@protonmail.com. Binance also provided a photograph that was provided by **Sheppard** to Binance which contains an image of **Sheppard** holding a driver's license in the name of **Mason John Sheppard**, which appears to be the same driver's license provided to Coinbase.

49. On July 21, 2020, federal agents executed a search warrant authorized by U.S. Magistrate Judge Alex G. Tse at a residence in the Northern District of California. Among the occupants of the home was a juvenile ("Juvenile 1"). "Juvenile 1" was believed to be a Discord user identified in chats as an individual who assisted "Kirk#5270" and "Chaewon" in selling access to Twitter accounts. Upon execution of the search warrant, "Juvenile 1" agreed to be interviewed. "Juvenile 1" admitted to law enforcement agents that he/she was the Discord user who was identified in chats as assisting "Kirk#5270" and that he/she participated in the sale of illegal Twitter access. "Juvenile 1" admitted that he/she worked with "**Chaewon**" to sell Twitter account access. According to "Juvenile 1," his/her knowledge of "**Chaewon**" was that "**Chaewon**" lived in the United Kingdom and "Juvenile 1" knew "**Chaewon**" by the name "**Mason.**" According to

“Juvenile 1,” he/she and “**Chaewon**” had discussed turning themselves in to law enforcement after the Twitter hack became publicly known.

IV. CONCLUSION

50. Based on the above information, I respectfully submit that there is probable cause to believe that **Mason John Sheppard**, also known as “**Chaewon**,” has:

- Aided and abetted intentional access of a protected computer and obtaining information, in violation of Title 18, United States Code, Section 1030(a)(2)(C) (Count One);
- Conspired with others to commit a violation of Title 18, United States Code, Section 1343 (wire fraud), in violation of Title 18, United States Code, Section 1349 (Count Two); and
- Conspired with others to commit money laundering, in violation of Title 18, United States Code, Section 1956(h) (Count Three).

FURTHER AFFIANT SAYETH NOT.

/s/Tigran Gambaryan via
telephone

Tigran Gambaryan
Special Agent
IRS-CI

Subscribed and sworn
before me on July 22, 2020



Honorable Alex G. Tse
United States Magistrate Judge