# UNITED STATES DISTRICT COURT

for the

Northern District of California



United States of America
v.

Nima Fazeli

*Defendant(s)*

Case No. 3:20-mj-71049 MAG

## 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 & elsewhere, the defendant(s) violated:

| *Code Section* | *Offense Description* |
|---|---|
| 18 U.S.C. § 1030(a)(2)(C) | Count One: Computer Intrusion<br><br>Max. Penalties: 5 years in prison; $250,000 fine; 3 years of supervised release; $100 special assessment; restitution; forfeiture |

This criminal complaint is based on these facts:

The attached affidavit of U.S. Secret Service SA John Szydlik

☑ Continued on the attached sheet.

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

/s/ J Szydlik via telephone
*Complainant's signature*

J. Szydlik, Special Agent, FBI
*Printed name and title*

Sworn to before me by telephone.

Date: 07/30/2020

*Judge's signature*

City and state: San Francisco, California

Hon. Sallie Kim, U.S. Magistrate Judge
*Printed name and title*

UNITED STATES DISTRICT COURT )

)

NORTHERN DISTRICT OF CALIFORNIA )

**AFFIDAVIT IN SUPPORT OF APPLICATION FOR AN ARREST WARRANT AND CRIMINAL COMPLAINT**

I, John A. Szydlik, being duly sworn, state as follows:

## OVERVIEW

1. This affidavit is made in support of an issuance of an arrest warrant and a one-count criminal complaint alleging that **Nima FAZELI**, also known as "**Rolex**," "**Rolex#0373**," "**Rolex#373**," and "**Nim F**," committed: Computer Intrusion, i.e., intentionally accessing a computer without authorization or exceeding authorized access, and thereby obtaining information from a protected computer, in violation of 18 U.S.C. § 1030(a)(2)(C) and aiding and abetting, in violation of 18 U.S.C. § 2. For the reasons set forth below, I believe there is probable cause to believe **Nima FAZELI** has committed the foregoing violations of federal law.

2. The facts in this affidavit come from my personal observations, my training and experience, information from records and databases, and information obtained from other agents, law enforcement personnel, and witnesses. This affidavit does not set forth all of my knowledge about this matter; it is intended to only show that there is sufficient probable cause for the requested arrest warrant and complaint.

## AFFIANT BACKGROUND

3. I am an investigative or law enforcement officer of the United States, within the meaning of 18 U.S.C. § 2510(7), and am empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in 18 U.S.C. § 1030, among others.

4. I am employed as a Special Agent with the United States Secret Service ("USSS") in Washington, D.C. and have been so employed since 2007. I am sworn and empowered to

investigate criminal activity involving violations of federal law. I am currently assigned to USSS's Criminal Investigative Division, Cyber Intelligence Section, which investigates crimes carried out using computers or computer networks. 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. My investigative experience includes, but is not limited to interviewing subjects, targets and witnesses; executing search and arrest warrants; handling and supervising confidential human sources; conducting surveillance; and analyzing phone records and financial records.

## APPLICABLE STATUTE

5. Title 18, United States Code, Section 1030(a)(2)(C), in relevant part, makes it a crime for an individual to intentionally access a computer without authorization or exceed authorized access, and thereby obtain information from a protected computer. Under Section 1030(c)(2)(B), the offense is a felony if "committed for purposes of commercial advantage or private financial gain," "committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State," or if "the value of the information obtained exceeds $5,000." A "protected computer" means a computer that is used in or affecting interstate or foreign commerce or communication (as defined by 18 U.S.C. § 1030(e)(2)(B)). Title 18, United States Code, Section 2, in relevant part, provides that whoever aids, abets, counsels, commands, induces, or procures the commission of a federal offense is punishable as a principal.

## DEFINITIONS

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

7. **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.

8. **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."

9. **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.

10. **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.

11. **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.

12. **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.

13. **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.

14. **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.

15. **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.

16. **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.

17. **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.

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

### A. TWITTER HACKED ON JULY 15, 2020

18. 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.

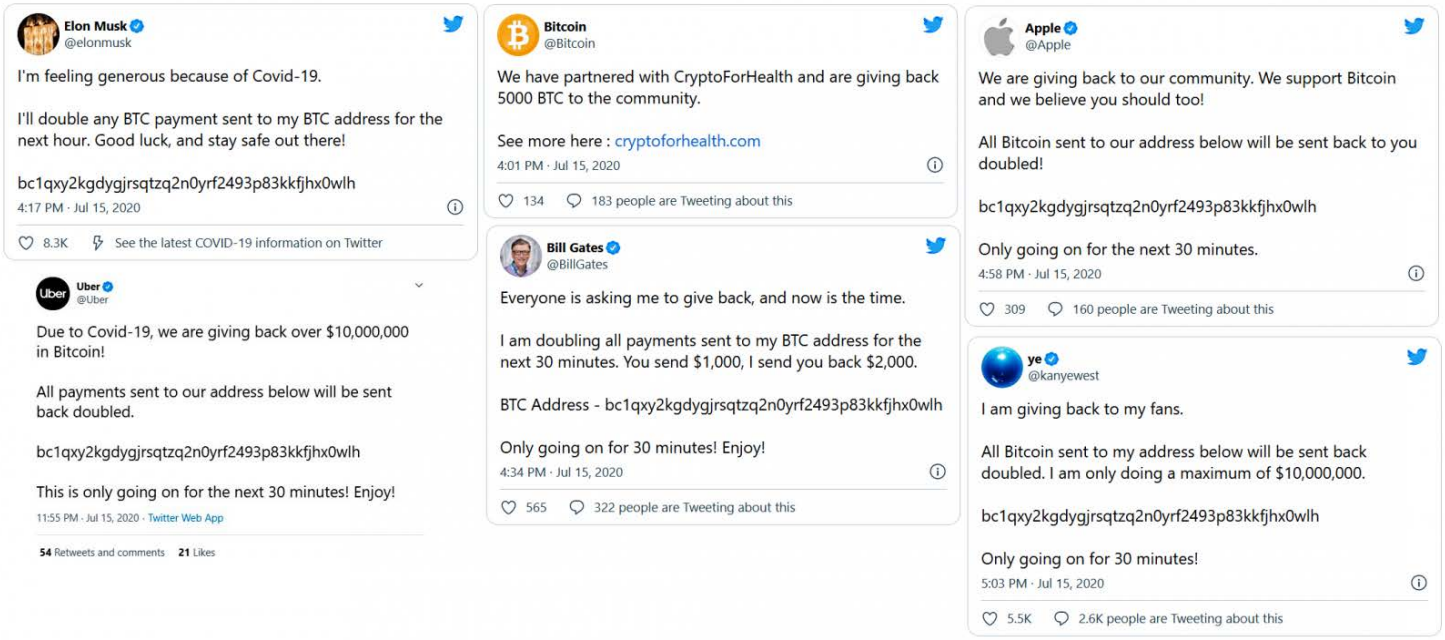
19. Per statements made by Twitter, numerous media reports, public victim statements, and through this investigation, on July 15, 2020, multiple high-profile verified accounts were compromised, including accounts belonging to Bill Gates, Elon Musk, Kanye West, Joe Biden, Barack Obama, Jeff Bezos, Mike 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 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."

20. 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."

21. 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 "bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh" (hereinafter, the "Scam Address"). Two other bitcoin addresses were also posted on some Twitter accounts: "bc1q0kznuxzk6d82e27p7gplwl68zkv40swyy4d24x" and "bc1qwr30ddc04zqp878c0evdrqfx564mmf0dy2w39l", which both received approximately $6,700 in 100 transactions. However, the primary bitcoin address known to be directly associated with the Twitter hack is the Scam Address.

22. 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 of these cases, the Twitter postings said that individuals who sent any bitcoin to the aforementioned address would receive double the bitcoin in return.

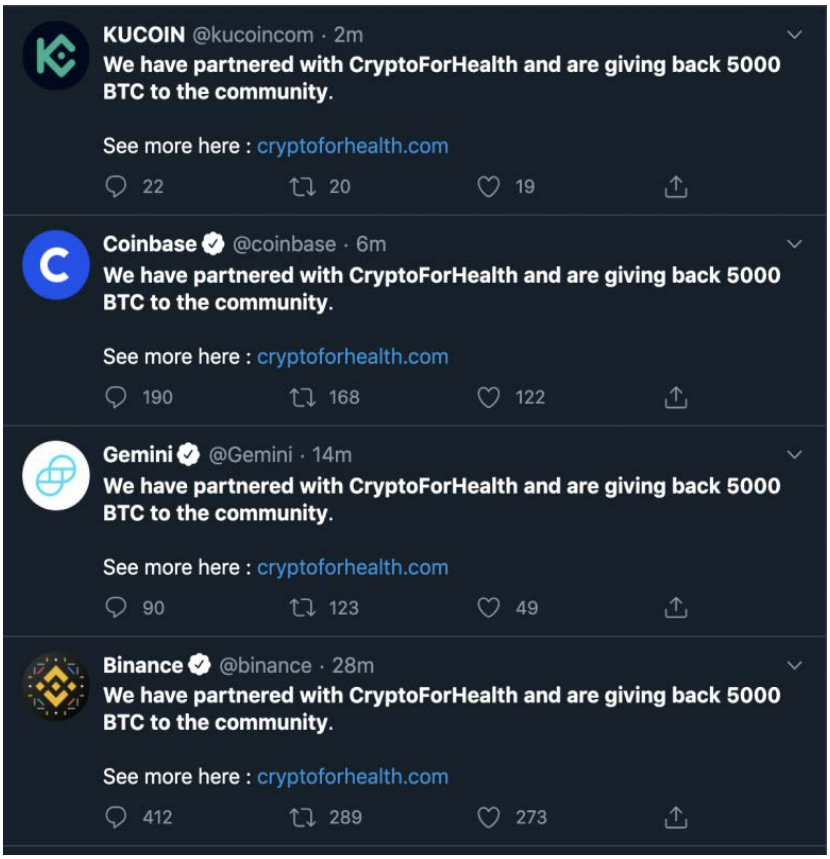
23. Below are screen captures of some of these Twitter posts from the compromised accounts belonging to Elon Musk, Bitcoin, Apple Kanye West, Bill Gates, and Uber:[1]




24. 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/.

25. 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]




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

27. The website hosted at cryptoforhealth.com led to a webpage that, like the other Twitter posts, directed individuals to send bitcoin to the bc1qxy 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).

28. 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]:


We believe that blockchain and Bitcoin will make the world more fair and open. The current financial system is outdated and COVID-19 has made serious damage to the traditional economy ,To help in these hard times For COVID19 Huobi, Kucoin, Kraken, Gemini, Binance, Coinbase & Trezor are partnered to give back to the community We decided to run 5000 BTC giveaway. To participate you just need to send from ~0.1 BTC to 20 BTC to the contribution address and we will immediately send you back 0.2 BTC to 40 BTC to the address you sent it from (x2 back).
Supported exchanges / wallets: Coinbase, Robinhood, Kraken, Binance, Blockchain, Gemini, Changelly, Bitstamp, Bittrex, CEX.io and many others.
You can participate only once!
SPECIAL OFFER:
If you send 0.1 - 0.19 BTC you will be airdropped 0.2 - 0.38 BTC back.
If you send 0.2 - 0.99 BTC you will be airdropped 0.4 - 1.98 BTC back +1% bonus.
If you send 1 - 4.99 BTC you will be airdropped 2 - 9.98 BTC back +5% bonus.
If you send 5 - 9.99 BTC you will be airdropped 10 - 19.98 BTC back +10% bonus.
If you send 10 - 19.99 BTC you will be airdropped 20 - 39.98 BTC back +20% bonus.
If you send 20 BTC you will be airdropped 40 BTC back +25% bonus.
CONTRIBUTION ADDRESS:
You can send BTC to the following address:
bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh
Copy Address to Clipboard
Instruction:
- To make a transaction, you can use any wallet or exchange to participate!
- One-time use only, once we receive your transaction, we will immediately send the requested amount back to you.
Waiting for payment
Still waiting for transaction? Click Here
Once we receive your transaction, the outgoing transaction is processed to your address.
Every address that is sent too late, gets their BTC immediately sent back.

29. 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.

30. I believe that the actors(s) who controlled the cryptoforhealth.com domain and the Scam 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 message posted

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

on the website hosted at the domain cryptoforhealth.com—in order to entice individuals into sending bitcoin to the Scam Address. The individual(s) then stole the bitcoin, and transferred it out of the account. (Further below, I will refer to this scheme as the "Bitcoin Scam.")

### B. TWITTER HACK PROCEEDS TRANSFERRED TO THE PRIMARY SCAM ADDRESS

31. Blockchain analysis reveals that between July 15, 2020, when the hack of the verified Twitter accounts occurred, and July 16, 2020, the bitcoin wallet associated with the Scam Address had conducted approximately 426 transfers.

32. Approximately 415 of those transfers consisted of transfers from other bitcoin addresses into the Scam Address 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 Scam Address to other bitcoin addresses, siphoning off approximately 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.

33. 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.

### C. KIRK#5270 SOLD ACCESS TO HACKED TWITTER ACCOUNTS

34. From the investigation, I have probable cause to believe that the individual utilizing the Discord moniker "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 the content of Discord messaging accounts, which included Discord chats between an individual utilizing the username "Kirk#5270"

[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.

and others, in which "Kirk#5270" represented that he/she could reset, swap, and control any Twitter account at will, and would do so in exchange for bitcoin transfers.

35. Among the content provided by Discord was a chat from July 15, 2020, between "Kirk#5270" and other Discord users in which "Kirk#5270" demonstrated 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.

36. Based on the chats that I have reviewed, it appears that "Kirk#5270" utilized other Discord users as proxies, or middle-men, to help "Kirk#5270" find buyers for Twitter usernames in exchange for a fee.

### D. ROLEX#0373 SERVED AS A PROXY FOR KIRK#5270 AND SOLD TWITTER ACCOUNTS

41. Among the content provided by Discord was a series of chats on July 15, 2020 between "Kirk#5270" and an individual who used the Discord moniker "Rolex#0373." "Kirk#5270" stated, "I work for Twitter. I can claim any @ for you."[5] Based on my training and experience, I believe that this reference by "Kirk#5270" was to being able to take control of any Twitter account and transfer control to "Rolex#0373" or others. "Rolex#0373" asked "Kirk#5270" to "Prove it," in response to which "Kirk#5270" asked for "Rolex#0373's" Twitter handle. "Rolex#0373" responded, providing the Twitter handle "viennacat921," and "Kirk#5270" replied by providing a screenshot of an internal Twitter panel for the Twitter handle "@viennacat921" with the associated email and phone number for the Twitter account. The following is an excerpt of the Discord chat:

| Date and Time | Message Sender | Message |
|---|---|---|
| 2020-07-15 17:20:33.243000 | Rolex#0373 | Yo |
| 2020-07-15 17:28:51.135000 | Kirk#5270 | Hey |

[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 a social media username.

| | | |
|---|---|---|
| 2020-07-15 17:28:55.093000 | Kirk#5270 | I work for twitter |
| 2020-07-15 17:29:02.307000 | Kirk#5270 | I can claim any @ for you. |
| 2020-07-15 17:29:03.448000 | Kirk#5270 | Let me know. |
| 2020-07-15 17:29:06.470000 | Kirk#5270 | Don't tell anyone. |
| 2020-07-15 17:29:17.161000 | Rolex#0373 | Lol |
| 2020-07-15 17:29:25.103000 | Rolex#0373 | Prove it |
| 2020-07-15 17:29:25.604000 | Kirk#5270 | Give me your twitter @ |
| 2020-07-15 17:29:50.665000 | Kirk#5270 | I'll pull it up |

| | | |
|---|---|---|
| 2020-07-15 17:30:23.536000 | Kirk#5270 | Give me your twitter @ |
| 2020-07-15 17:30:27.461000 | Rolex#0373 | viennacat921 |
| 2020-07-15 17:30:31.573000 | Kirk#5270 | Yours? |
| 2020-07-15 17:30:33.221000 | Rolex#0373 | Yes |

42. Upon receiving the image of the internal tool showing information associated with the "@viennacat921" Twitter moniker, "Rolex#0373" asked whether "Kirk#5270" could change information on the account. "Kirk#5270" clarified that he/she could "update any info" and "delete account data." "Rolex#0373" then asked "Kirk#5270" how much it would cost, and "Kirk#5270" responded that it depended on the Twitter moniker ("@"). "Rolex#0373" offered to serve as a "proxy" for "Kirk#5270" and advertise on various internet forums, stating, "I could also proxy sell requests for you on forums." "Kirk#5270" responded that "Rolex#0373" should "do that" and to "post a thread." The following is an excerpt of the Discord chat:

| Date and Time | Message Sender | Message |
|---|---|---|
| 2020-07-15 17:31:09.628000 | Rolex#0373 | Damn |
| 2020-07-15 17:31:20.276000 | Rolex#0373 | So you can change info? |
| 2020-07-15 17:31:27.301000 | Kirk#5270 | Yes can update any info |
| 2020-07-15 17:31:31.065000 | Kirk#5270 | And I delete account data |
| 2020-07-15 17:31:36.674000 | Kirk#5270 | So no recovery |
| 2020-07-15 17:31:37.784000 | Kirk#5270 | Or logs |
| 2020-07-15 17:31:40.224000 | Rolex#0373 | How much for requests |
| 2020-07-15 17:31:47.193000 | Kirk#5270 | Depends on @ |
| 2020-07-15 17:31:49.858000 | Kirk#5270 | What @ do you want rn |
| 2020-07-15 17:32:20.154000 | Rolex#0373 | I could be interested in a few depending on the price |
| 2020-07-15 17:32:25.234000 | Rolex#0373 | None of them would be super OG |

| | | |
|---|---|---|
| 2020-07-15 17:33:36.308000 | Rolex#0373 | I could also proxy sell requests for you on forums |
| 2020-07-15 17:33:43.664000 | Kirk#5270 | Okay |
| 2020-07-15 17:33:44.377000 | Kirk#5270 | Do that |
| 2020-07-15 17:33:45.717000 | Kirk#5270 | Post a thread |
| 2020-07-15 17:34:00.540000 | Rolex#0373 | Alr |

43. During the course of the chat between "Rolex#0373" and "Kirk#5270," "Kirk#5270" provided "Rolex#0373" with access to the Twitter handle "@foreign" in exchange for $500. "Kirk#5270" asked "Rolex#0373" for his email address in order to reset the Twitter account associated with the "@foreign" handle, and "Rolex#0373" provided the email "chancelittle10@gmail.com." "Kirk#5270" responded by providing a bitcoin address: "1Ai52Uw6usjhpcDrwSmkUvjuqLpcznUuyF" (hereinafter, the "Kirk#5270 Address") to "Rolex#0373." Based on my training and experience, I understand that "kirk#5270" was offering to change the email address on the "@foreign" handle to "chancelittle10@gmail.com" in exchange for a payment to the Kirk#5270 Address. "Rolex#0373" responded by stating that he had not agreed to "buy it" but asked if he could "keep it" in exchange for "Rolex#0373" selling Twitter handles for "Kirk#5270." The following is an excerpt of the Discord chat:

| Date and Time | Message Sender | Message |
|---|---|---|
| 2020-07-15 17:43:23.831000 | Kirk#5270 | 500 for foreign |
| 2020-07-15 17:43:30.176000 | Kirk#5270 | lowest ill go |
| 2020-07-15 17:43:30.964000 | Kirk#5270 | for this |
| 2020-07-15 17:43:36.017000 | Kirk#5270 | I'll update them eail |
| 2020-07-15 17:43:39.216000 | Kirk#5270 | that you give me |
| 2020-07-15 17:43:53.633000 | Rolex#0373 | Check the last login date |
| 2020-07-15 17:43:54.438000 | Rolex#0373 | for it |
| 2020-07-15 17:44:27.132000 | Kirk#5270 | |
| 2020-07-15 17:44:32.993000 | Kirk#5270 | 1 year ago |
| 2020-07-15 17:45:58.930000 | Rolex#0373 | Can't even be swapped |
| 2020-07-15 17:46:03.207000 | Kirk#5270 | Yes |
| 2020-07-15 17:46:03.725000 | Kirk#5270 | Lol |
| 2020-07-15 17:46:04.079000 | Kirk#5270 | Bro |
| 2020-07-15 17:46:24.962000 | Rolex#0373 | Just sounds too good to be true |
| 2020-07-15 17:46:29.439000 | Kirk#5270 | Ok |
| 2020-07-15 17:46:31.039000 | Kirk#5270 | Give me your email |

| | | |
|---|---|---|
| 2020-07-15 17:46:40.408000 | Rolex#0373 | chancelittle10@gmail.com |
| 2020-07-15 17:47:22.154000 | Kirk#5270 | Reset through forgot |
| 2020-07-15 17:48:15.018000 | Rolex#0373 | I'm in |
| 2020-07-15 17:48:28.318000 | Kirk#5270 | 1Ai52Uw6usjhpcDrwSmkUvjuqLpcznUuyF |
| 2020-07-15 17:48:32.257000 | Rolex#0373 | Bruh |
| 2020-07-15 17:48:54.616000 | Rolex#0373 | I didn't say I'd buy it lol |
| 2020-07-15 17:49:02.221000 | Rolex#0373 | Just lemme keep it and I'll open the service? |
| 2020-07-15 17:49:11.572000 | Rolex#0373 | And we can charge like 1k a req |
| 2020-07-15 17:49:16.667000 | Kirk#5270 | Ok |

44. During the chat between "Kirk#5270" and "Rolex#0373," "Kirk#5270" directed "Rolex#0373" to post a thread on online forums advertising Twitter handles and to "start hitting up your contacts." "Kirk#5270" and "Rolex#0373" then discussed pricing for the sale of unauthorized access to the Twitter accounts. "Kirk#5270" and "Rolex#0373" agreed on $1,000 per account at a minimum for non-"OG" names and $2,500 minimum for "OG," names, referring to short "original" or "OG" Twitter handles that are seen as status symbols and are desirable handles. "Rolex#0373" provided "Kirk#5270" with a hyperlink to a thread on the OGUsers.com ("OGUsers") forum for advertising the sale of Twitter handles. Based on my training and experience, the OGUsers forum is abused by criminal networks, as further discussed below. The following is an excerpt of the Discord chat:

| Date and Time | Message Sender | Message |
|---|---|---|
| 2020-07-15 17:49:16.667000 | Kirk#5270 | Ok |
| 2020-07-15 17:49:17.596000 | Kirk#5270 | Open it now |
| 2020-07-15 17:49:18.155000 | Kirk#5270 | Then |
| 2020-07-15 17:49:20.616000 | Rolex#0373 | Alr |
| 2020-07-15 17:49:24.329000 | Rolex#0373 | On ogu or hf |
| 2020-07-15 17:49:25.870000 | Kirk#5270 | And start hitting up your contacts |
| 2020-07-15 17:49:26.759000 | Kirk#5270 | Both |
| 2020-07-15 17:49:32.067000 | Rolex#0373 | Ight |
| 2020-07-15 17:49:48.095000 | Rolex#0373 | 1k per req? |
| 2020-07-15 17:49:51.597000 | Kirk#5270 | No |
| 2020-07-15 17:49:51.925000 | Rolex#0373 | Active & inactive? |
| 2020-07-15 17:49:52.642000 | Kirk#5270 | Appraisal |

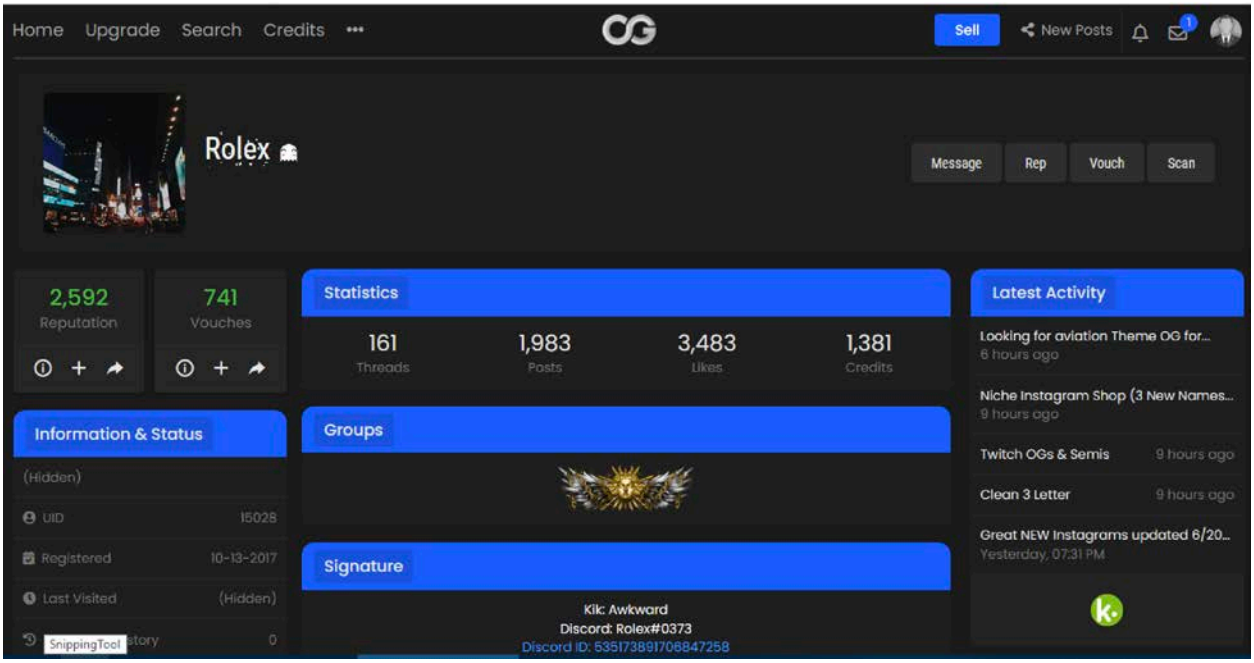
| | | |
|---|---|---|
| 2020-07-15 17:49:55.667000 | Kirk#5270 | Yes |
| 2020-07-15 17:49:56.855000 | Rolex#0373 | Ight |
| 2020-07-15 17:54:35.673000 | Rolex#0373 | I'm gonna say 1k minimum |
| 2020-07-15 17:54:38.559000 | Rolex#0373 | cool? |
| 2020-07-15 17:54:40.049000 | Kirk#5270 | Yep |
| 2020-07-15 18:07:55.181000 | Rolex#0373 | https://ogusers.com/Thread-Twitter-Username-Requests--618499 |
| 2020-07-15 18:08:33.500000 | Rolex#0373 | I put 1k minmimum |
| 2020-07-15 18:08:36.422000 | Rolex#0373 | Let's say that's for non-og |
| 2020-07-15 18:08:39.918000 | Rolex#0373 | 2.5k minimum for og? |
| 2020-07-15 18:09:47.411000 | Kirk#5270 | 1k min for all |
| 2020-07-15 18:09:48.176000 | Kirk#5270 | is fine |
| 2020-07-15 18:09:54.081000 | Rolex#0373 | Alr |

45. In summary, based on the facts described above, as well as my training and experience, I believe that "Rolex#0373" acted as a broker for "Kirk#5270," and advertised the sale of compromised Twitter accounts for "Kirk#5270" and procured buyers for "Kirk#5270."

### E. DISCORD USER "ROLEX#0373" IDENTIFIED AS "ROLEX" ON OGUSERS FORUM

46. OGUsers is an online forum that has been abused by criminal networks who trade in stolen social media credentials. On April 2, 2020, the administrator of OGUsers publicly announced the OGUsers website was successfully hacked. Shortly after the announcement, a rival criminal hacking forum publicly released a link to download the OGUsers 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. A review of the OGUsers database reveals that it contains communications up until March 31, 2020 and are consistent with other sources of data that overlap it. To my knowledge there have been no instances where the OGUsers database appears to have been altered by whomever leaked it.

47. Through a search of the OGUsers database, I identified an individual with the username "Rolex" who registered on the forum with the email address "damniamevil20@gmail.com" and accessed the account from IP address 104.51.181.242 which appears to resolve to Florida. On March 30, 2020, on the OGUsers forum, "Rolex" told another individual, "Confirming I'm Rolex#0373." I believe that "Rolex" was referring to his Discord account, "Rolex#0373". Additionally, as demonstrated in the below screenshot of "Rolex's" profile on OGUsers from July 30, 2020, he provides the Discord user name "Rolex#0373."




48. On several occasions in the OGUsers forum, "Rolex" advertised a "Currency Exchange Service" where he claimed to be able to convert Bitcoin to the Paypal online payments service and various cyptocurrencies. Rolex also advertised the sale of various social media accounts.

49. Additionally, through a review of the OGUsers database, I am aware that "Rolex" provided the email address "chancelittle10@gmail.com" as a method of sending him PayPal payments on multiple occasions to multiple users of the OGUsers forum in 2018. Notably, this is the same email address that "Rolex#0373" provided "Kirk#5270" in order to obtain access to the Twitter handle "@foreign" during the July 15, 2020 hack of Twitter.

### F. ROLEX#0373 and "ROLEX" LINKED TO NIMA FAZELI

50. There is probable cause to believe that **Nima FAZELI** is the user of Discord account "Rolex#0373" and OGUsers account "Rolex," in part, based on several IP addresses that were used to access both the Discord account "Rolex#0373" and OGUsers account "Rolex," and based on Coinbase records associated with "Rolex."

51. On October 30, 2018, an individual on the OGUsers forum asked "Rolex" to exchange $25 in PayPal funds for $20 in Bitcoin and provided the Bitcoin address "1PkwTmn3Eo48oLqE9w4MFckDQmgzq69u1f" (hereinafter, "1Pkw Address") for "Rolex" to send the funds. Based on records from Coinbase, a cryptocurrency exchange, on October 30, 2018, an account in the name of "**Nim F**" sent approximately $20 to the 1Pkw Address. The "**Nim F**" account was created on December 23, 2017, and was later closed (hereinafter "**FAZELI** Coinbase Account 1"). Coinbase records revealed that the "**Nim F**" account was registered with the email address "damniamevil20@gmail.com," which matches the registered email address for "Rolex" on the OGUsers forum. Additionally, the accountholder for the "**Nim F**" account used a Florida driver's license with a number ending in 300-0 and in the name of **Nima FAZELI** to verify the account. According to Florida DMV officials, this driver's license is a legitimate driver's license associated with **Nima FAZELI.** On multiple occasions, the "**Nim F**" account transacted with the another Coinbase account in the name of "**Nima FAZELI**," which was registered to the email address "nimafazeli20@yahoo.com" (hereinafter, "**FAZELI** Coinbase Account 2"). The same **FAZELI** driver's license was used to verify FAZELI Coinbase Account 2.

52. Similarly, on multiple occasions between October 11, 2019, and March 17, 2020, "Rolex" provided the bitcoin address 3Aieac9YpxmWkWmRcQNUSMjDSswYxnHZps (hereinafter, "3Aie Address") to multiple other OGUsers accountholders in order for those individuals to send payments or conduct money exchanges via "Rolex." Based on records from Coinbase, the 3Aie Address was assigned to an account in the name of "**Nima FAZELI**," which was registered to the email address "nima.fazeli@yahoo.com" (hereinafter, "**FAZELI** Coinbase Account 3"). This particular account was created on June 24, 2017, and it was verified using the

Florida driver's license of **Nima FAZELI**. This driver's license is the same license that was used to verify FAZELI Coinbase Account 1 and FAZELI Coinbase Account 2, and, based on information from the Florida DMV officials, it is associated with **Nima FAZELI**. As of July 30, 2020, the **FAZELI** Coinbase Account 3 had approximately 1,900 transactions totaling approximately 21.46 Bitcoin, worth approximately $237,551 as of July 30, 2020.

53. The investigation shows that the **FAZELI** Coinbase Account 3 and the "Rolex#0373" Discord were accessed from the same IP addresses. These IP addresses are 104.51.181.242 and 107.145.123.179. According to a reliable public IP geolocation service named MaxMind, IP address 104.51.181.242 is registered to AT&T based in Orlando, FL and IP address 107.145.123.179 is registered to Spectrum in Rockledge, FL.

a. IP address 104.51.181.242 accessed the **FAZELI** Coinbase Account 3 on multiple occasions from August 5, 2019, to May 5, 2020. The same IP address was used to access the "Rolex#0373" Discord account on multiple occasions from January 20, 2020, to July 17, 2020. On several occasions, the same IP address was used to access both accounts on the same day including on January 29, 2020, March 12, 2020, March 16, 2020, and May 5, 2020; and

b. IP address 107.145.123.179 accessed the "Rolex#0373" Discord account on multiple occasions from February 1, 2020, to June 6, 2020. The IP address also accessed the **FAZELI** Coinbase Account 3 on multiple occasions from July 4, 2019 to June 6, 2020. The IP address accessed both accounts on March 20, 2020.

54. Based on my training and experience, as the **FAZELI** Coinbase Account 3 and the "Rolex#0373" Discord account and the "Rolex" OGUsers account were accessed from the same IP address on several occasions, I believe that they are controlled by the same person.

55. Based on the above information, and in particular that the **FAZELI** Coinbase Account 2 and the **FAZELI** Coinbase Account 3 were registered in the name of **Nima FAZELI**, and all three Coinbase accounts were established using **Nima FAZELI**'s driver's license, I believe that that **FAZELI** controls both the "Rolex#0373" Discord account the "Rolex" OGUsers account.

## CONCLUSION

56. For the reasons set forth above, I believe that there is probable cause that **Nima FAZELI** intentionally accessed the computer(s) of Twitter and thereby obtained information from a protected computer, without the authorization of Twitter or applicable Twitter accountholders, or aided and abetted others in doing so, in violation of 18 U.S.C. §§ 1030(a)(2)(C) and 2.

/s/ John Szydlik via telephone
John Szydlik
Special Agent
United States Secret Service

Sworn to before me over the telephone and signed by me pursuant to Fed. R. Crim. P. 4.1 and 4(d) on this 30 day of July, 2020. This application and warrant are to be filed under seal.

HONORABLE SALLIE KIM
United States Magistrate Judge