AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

District of Connecticut

United States of America
v.

MICHAEL RICHO

Defendant(s)

Case No. 3:16-mj-464 (SALM)

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 November 2013 to October 2014 in the county of New Haven in the District of Connecticut, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. §§ 1029(a)(2) and (a)(3)	Access device fraud
18 U.S.C. §§ 1030(a)(2) and (a)(4)	Computer fraud
18 U.S.C. § 1343	Wire fraud
18 U.S.C. § 1028A	Aggravated identity theft
18 U.S.C. § 1956(a)(1)(B)(i)	Money laundering

This criminal complaint is based on these facts:

See attached Affidavit of FBI Specel Agent Michael Morrison, which is incorporated herein by reference.

☑ Continued on the attached sheet.

Complainant's signature

Michael Morrison, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 10/03/2016

/s/ Sarah A. L. Merriam

Judge's signature

City and state: New Haven, CT

Sarah A. L. Merriam, U.S. Magistrate Judge

Printed name and title

3:16mj 464-SALM

STATE OF CONNECTICUT : **UNDER SEAL**

: ss: New Haven, Connecticut

COUNTY OF NEW HAVEN : October 3, 2016

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT AND ARREST WARRANT

I, Michael Morrison, being duly sworn, depose and state as follows:

BACKGROUND OF AFFIANT

1. I have been employed as a Special Agent for the Federal Bureau of Investigation ("FBI") since 2012. I am currently assigned to the cybercrime squad of the New Haven Division. I have received training and gained experience in, *inter alia*, arrest procedures, search warrant applications, the execution of searches and seizures, computer crimes, and computer evidence identification, seizure and processing. I have personally participated in investigations related to financial fraud, cybercrimes, and cyber intrusions. In addition to my work experience, I have received specialized training in the field of computer crime investigation from the FBI and others. I am an "investigative or law enforcement officer of the United States," within the meaning of 18 U.S.C. § 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in 18 U.S.C. § 2516.

2. I make this affidavit in support of a Criminal Complaint and Arrest Warrant charging Michael Richo ("RICHO"), a 34-year old male born in 1981 and having a social security number of xxx-xx-0169, with access device fraud, in violation of 18 U.S.C. §§ 1029(a)(2) and (a)(3), computer fraud, in violation of 18 U.S.C. §§ 1030(a)(2) and (a)(4), wire fraud, in violation of 18 U.S.C. § 1343, aggravated identity theft, in violation of 18 U.S.C. § 1028A, and money laundering, in violation of 18 U.S.C. § 1956(a)(1)(B)(i) (collectively, the "TARGET OFFENSES"). Based on the facts set forth below, I believe there is probable cause to believe, and

I do believe, that RICHO knowingly committed the TARGET OFFENSES in the District of Connecticut.

3. The statements contained in this affidavit are based in part on information provided by other members of local, state, and federal law enforcement, my own investigation to include personal observations, documents and other investigative materials which I have reviewed, as well as my training and experience as a Special Agent with the FBI. Since this affidavit is being submitted for the limited purpose of obtaining a criminal complaint and arrest warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that RICHO committed the TARGET OFFENSES.

RELEVANT STATUTES

4. This investigation concerns possible violations of 18 U.S.C. §§ 1029 (access device fraud), 1030 (computer fraud), 1343 (wire fraud), 1028A (aggravated identity theft), and 1956 (money laundering).

5. 18 U.S.C. § 1029(a)(2) prohibits a person from knowingly, and with intent to defraud, using one or more unauthorized access devices during any one-year period and by such conduct, obtaining anything of value aggregating $1,000 or more during that period. 18 U.S.C. § 1029(a)(3) further prohibits a person from knowingly, and with intent to defraud, possessing fifteen or more unauthorized access devices. The term "access device" is defined to mean, among other things, any card, account number, electronic serial number, personal identification number, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds. The term "unauthorized access device" is defined to mean any access device

that is, among other things, stolen or expired with intent to defraud.

6. 18 U.S.C. § 1030(a)(2) (computer fraud) prohibits a person from, among other things, accessing a computer without authorization, and thereby obtaining information from a protected computer. 18 U.S.C. § 1030(a)(4) further prohibits a person from knowingly and with intent to defraud, accessing a protected computer without authorization, and by means of such conduct furthering the intended fraud and obtaining anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any one-year period. The term "protected computer" is defined to include, among other things, a computer used in or affecting interstate or foreign commerce or communication.

7. 18 U.S.C. § 1343 (wire fraud) prohibits a person who, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice.

8. 18 U.S.C. § 1028A (aggravated identity theft) prohibits a person, during and in relation to certain enumerated felonies, from knowingly transferring, possessing, or using, without lawful authority, a means of identification of another person. The enumerated felonies include any violations of Chapters 47 and 63, which, in turn, includes violations of 18 U.S.C. §§ 1029 (access device fraud), 1030 (computer fraud), and 1343 (wire fraud). The term "means of identification" is defined to include, among other things, any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including, among other things, a name, social security number, or unique electronic identification number or

address. The term "means of identification" also includes an "access device" as defined in 18 U.S.C. § 1029.

9. 18 U.S.C. § 1956(a)(1)(B)(i) prohibits a person from conducting or attempting to conduct a financial transaction involving proceeds of specified unlawful activity in order to conceal or disguise the nature, location, source, ownership or control of such proceeds. The term "conducts" is defined to include initiating, conducting, or participating in initiating, or concluding a transaction. The term "specified unlawful activity" includes violations of 18 U.S.C. §§ 1029 (access device fraud), 1030 (computer fraud), and 1343 (wire fraud).

BACKGROUND ON BITCOINS

10. Bitcoins are an anonymous, decentralized form of electronic currency, existing entirely on the Internet and not in any physical form. The currency is not issued by any government, bank, or company, but rather is generated and controlled automatically through computer software operating on a "peer-to-peer" network. Bitcoin transactions are processed collectively by the computers composing the network. To acquire bitcoins in the first instance, a user typically must purchase them from a bitcoin "exchanger," who accepts payments of currency in conventional form, and exchanges them for bitcoins, based on a fluctuating exchange rate. Bitcoins are maintained by a user in an electronic "wallet," associated with a bitcoin "address," which is analogous to an account number for a bank account. A user can use bitcoins in his wallet to conduct financial transactions by transferring bitcoins from his bitcoin address to the bitcoin address of another user. The "address" is analogous to the account number for a bank account, while the "wallet" is analogous to a bank safe where the money in the account is physically stored. All bitcoin transactions are maintained on a public ledger known as the "Blockchain," which serves to prevent a user from spending the same bitcoins more than once. However, the Blockchain only

reflects the movement of funds between anonymous bitcoin addresses and therefore cannot by itself be used to determine the identities of the persons involved in the transactions.

11. There are a number of online exchanges that allow users to buy and sell bitcoins for fiat currency, such as U.S. currency. In addition, there are online services that allow users to exchange their bitcoins directly with other users. One such service is Local Bitcoins, which is located on the internet at http://localbitcoins.com. According to the Local Bitcoins website, "LocalBitcoins.com is a person-to-person bitcoin trading site. At LocalBitcoins.com, people from different countries can exchange their local currency to bitcoins. The site allows users to post advertisements where they state exchange rate and payment methods for buying or selling bitcoins."

12. A bitcoin tumbler is a mixing service which is utilized to help mask the trail of bitcoins. Since all bitcoin transactions are documented on the Blockchain, a tumbler attempts to mask the transactional trail by having a person send their bitcoins to this service, often for a nominal fee, which then will combine them with many other people's bitcoins. The service, over a period of time and multiple random transactions will send the bitcoins to a new bitcoin address in the control of the mixing service's client. Based on my training and experience and information provided to me by others, I am aware that Bitcoin Fog is an online bitcoin tumbling service.

BACKGROUND ON TOR AND THE "DARK WEB"

13. "Tor," which is an acronym for "The Onion Router," is a special network of computers on the Internet, distributed around the world, that is designed to conceal the true IP addresses[1] of the computers on the network, and, thereby, the identities of the network's users.

[1] Every computer device connected to the Internet has an "Internet protocol" or "IP" address assigned to it, which is used to route Internet traffic to or from the device. A device's IP address can be used to determine the device's physical location and, thereby, its user.

Every communication sent through Tor is bounced through numerous relays within the network, and wrapped in numerous layers of encryption, such that it is practically impossible to trace the communication back to its true originating IP address. Tor likewise enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites. Such "hidden services" operating on Tor have complex web addresses, generated by a computer algorithm, ending in ".onion" (rather than ".com" or ".net"). In order to access the Tor network, anyone can simply download the Tor browser software and use it to access the internet. Because of the anonymity provided to users and websites on the Tor network, it is sometimes referred to as the "Dark Web."

14. Based on my training and experience, I am aware that criminals have taken advantage of the Dark Web to create websites with online marketplaces dedicated to the trafficking of controlled substances and other illicit goods. Many of these online marketplaces further protect the anonymity of their users by requiring all transactions to be paid for through the use of bitcoins. Typically, in order to make purchases of products from these online marketplaces, a user must first obtain bitcoins and send them to his or her account at the online marketplace. The marketplace maintains information regarding the balance of bitcoins maintained by each user. After funding his or her account, the user can then make purchases from the marketplace. When the user purchases an item on the marketplace, the bitcoin balance of the user is debited by the purchase price. The purchase price is held in escrow by the marketplace, and after the sale is completed, the marketplace releases the bitcoins from escrow. Users can withdraw bitcoins from their bitcoin balances on the marketplace by providing the marketplace with a bitcoin address to which funds can be transferred. Some marketplaces charge a commission for every transaction conducted by its users.

THE INVESTIGATION AND PROBABLE CAUSE

15. In November 2013, the FBI began investigating RICHO in connection with his involvement with a hidden online marketplace on the Tor network that specialized in the sale of illegal narcotics, stolen credit cards, and other illicit items. The FBI subsequently obtained information that RICHO may have been involved in an online phishing[2] scheme whereby RICHO would obtain people's usernames and passwords in an effort to steal their bitcoins. At the time, RICHO was living in West Haven, Connecticut.

16. On November 4, 2014, the Honorable Holly B. Fitzsimmons, United States Magistrate Judge for the District of Connecticut, issued a federal search and seizure warrant for RICHO's residence in West Haven. I was the affiant in the application for that search warrant.

17. FBI agents and other law enforcement officers executed the warrant on November 6, 2014. I was not present during the execution of the warrant, but I have reviewed reports related to the execution of the warrant.

18. During the execution of the warrant, FBI agents and other law enforcement officers located and seized multiple computers, external hard drives, and thumb drives.

19. As the search was being executed, RICHO agreed to an interview with FBI agents at his residence. During the interview, RICHO admitted, in substance and in part, the following:

a. RICHO has his own business called MediaPen.

---

[2] Phishing is an attempt by a person to learn information such as login credentials or account information of another individual by impersonating a reputable entity or person via emails, websites, or other communication channels. Often times, a person operating a phishing scheme will create emails that appear to be from a legitimate entity, such as a bank for example. The email may ask the recipient to respond with account login credentials, or it may contains links to what appears to be the entity's website, but in reality, it is a fake website that is designed to capture an individual's login credentials.

b. RICHO steals bitcoins from users and vendors trying to access online marketplaces on the Tor network.

c. RICHO used two types of scams to steal user's login information to these sites. He would post fake links on forums to these markets which would direct users to a fake login page hosted on a laptop at his house. The login page would look exactly like the real login pages for the various market sites. When users would attempt to log in, he would steal their usernames and passwords.

d. The other technique RICHO used to steal login credentials involved posting fake links on forums that when clicked would "port forward" the users through RICHO's computer server to the actual marketplace site where users would log in. RICHO would keylog[3] all of the user's traffic including their login information.

e. Once RICHO had access to a user's account, he would use a program called "bitcoin monitor" to notify him when a deposit was made into the user's bitcoin wallet. After receiving notification of a deposit, he would log in to the account and withdraw the bitcoins before the user could spend them. He would often use "Bitcoin Fog" when transferring the bitcoins to hide his trail. The bitcoins would then be deposited into his bitcoin wallet with "Local Bitcoins" where he would sell them in exchange for cash deposits into his Bank of America account, Green Dot prepaid debit cards, Western Union transfers, or Money Gram transfers. RICHO's username with Local Bitcoins was "bmerc."

f. RICHO estimated that he had stolen over "six figures" worth of bitcoins.

[3] Keylogging, sometimes referred to as keystroke logging, is the action of recording (logging) the keys struck on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored.

g. RICHO stated he had a program on his laptop that stored the stolen usernames and passwords in a file called "nicefancy.txt." RICHO believed it currently had over 10,000 lines of text.

20. During the interview, RICHO also advised FBI agents that he had additional computer hard drives in a safety deposit box at People's United Bank. RICHO signed a consent to search form allowing the FBI to search and seize the contents of his safety deposit box, and he provided FBI agents with the key to his safety deposit box. FBI agents subsequently visited People's United Bank and seized the contents of RICHO's safety deposit box, which contained, among other things, a hard drive and thumb drives.

21. FBI computer forensic examiners subsequently examined the computers and hard drives seized from RICHO's residence and safety deposit box. I have reviewed the files recovered from the forensic examination. Among the files recovered from RICHO's computers and hard drives were dozens of files created between November 2013 and October 2014 that contain what appear to be thousands of usernames and passwords. I observed numerous files titled "nicefancy" followed by a date. For example, one file titled "nicefancy0929.txt" had a created date of September 29, 2014. The file contained what appear to be over 10,000 usernames and passwords. Based on my training and experience, my investigation to date, and RICHO's statements to law enforcement officers, I believe these are usernames and passwords belonging to other individuals that RICHO stole through the methods he described in his interview.

22. During the forensic examination, FBI computer forensic examiners also recovered numerous online chats between someone with usernames "fatfreak82828" and "fatfreak82829" and other individuals. In one of the chats, "fatfreak82828" asks another individual to email him at "mediapenllc@gmail.com." In another chat, one of the participants asks,

"mediapenllc@gmail.com[.] who is?? u?" to which fatfreak82829 replies, "me". As discussed, RICHO told law enforcement he has a business named Media Pen. I have reviewed online records from the Connecticut Secretary of State's website indicating that RICHO is the manager of MediaPen LLC. In addition, I have obtained and reviewed bank records for MediaPen LLC at Bank of America which lists RICHO as the manager of MediaPen LLC. I have also obtained and reviewed records from Green Dot Bank for prepaid debit cards registered to RICHO which indicate he registered one card using an email address mediapenllc@gmail.com. Based on this information, I believe that "fatfreak82828" and "fatfreak82829" are both RICHO.

23. In the chats, "fatfreak82828" admits to using a phishing scheme to steal individuals' login credentials in order to steal their bitcoins, and further admits he is an experienced computer hacker who has been hacking computers since he was 12 years old. The following are examples of some of the chat messages sent by "fatfreak82828," who I believe is RICHO, that were recovered from the forensic examination of RICHO's computers and hard drives:

a. On November 30, 2013, "fatfreak82828" wrote "i make my own phishing sites for darknet .onion drug sites[.] i make $1000 a day[.]"

b. Later in the same conversation, "fatfreak82828" sent the other chat participant the username, password, and bitcoin address of another individual and wrote "see those[?] username, passwor [sic], pin, balance, and all BTC[4] deposit addresses to a private illegal site . . . when i detect BTC payment there, i login, and withdraw[.] make $1000 day[.] all off 1 phishing site i built myself[.] so i know, how to do this, big time[.] i am prettty big too, but within TOR network[.]"

[4] BTC is an abbreviation for bitcoin.

c. On December 26, 2013, "fatfreak82828" wrote "i've been in hacking game hmm 15 years and before internet 5 years[.] when i was 12 years old i had police called on me for hacking bbs[.][5] 16 [years old] fbi raided my work i ran shellbox in the basement[.]"

d. Later in the same conversation, "fatfreak82828" wrote "i have 5000 l/p's[6] to darknet sites . . . . i live in a house by myself by the beach drive Mercedes all paid by :) . . . . i'd like to pass my business on and do other work but theres $500,000 a year to be made here[.] im making $30,000 a month[.] $5,000 a week or so[.]" At another point in the conversation, the other chat participant asked "fatfreak82828" what he does to make money, and "fatfreak82828" responded "phish but on darknet websites[.] i set up phish's scam pages for secret web pages[.]"

e. On December 27, 2013, "fatfreak82828" wrote "i have 5000 l/p's to illegal websites that deal in bitcoin[.] so i write scanners, that beat captcha, and login as each user[.] then i monitor each adddress and withdraw when they deposit[.] . . made $8700 in 1 minute once[.]"

f. Later in the same conversation, "fatfreak82828" wrote "i also have much experience with exploits, scanning, etc, rooting boxes, backdoors[.] i am building a botnet,[7] for windows . . . last time i ran botnet i had 2000 hosts join in 1 day." He further wrote "i do all my work over TOR[.] most of my attacks are on hidden sites within TOR[.] i run phishing sites that mimick other TOR sites[.] . . . i am writing something new, a botnet, for keylogging, etc."

---

[5] BBS is an abbreviation for bulletin board system.

[6] Based on my training and experience, I believe "l/p" is short for logins and passwords.

[7] Based on my training and experience, I am aware that a botnet is an interconnected network of computers infected with malware without the computer users' knowledge and controlled by cybercriminals. They are typically used to send spam emails, transmit viruses and engage in other acts of cybercrimes.

24. In the course of my investigation, I obtained and reviewed records from Local Bitcoins for the username "bmerc" which RICHO stated was his username. The records state the account holder's real name is "Michael Richo" and his email address is mediapenllc@gmail.com.

25. In my review of the records provided by Local Bitcoins, I observed hundreds of bitcoin transactions during the period from September 2013 to November 2014, including sales of bitcoins to other individuals in exchange for U.S. currency. I also obtained and reviewed bank records for MediaPen LLC at Bank of America and observed numerous deposits of U.S. currency, some of which correspond to the bitcoin sales I observed in the records from Local Bitcoins. For example, I observed the following transactions in the records provided by Local Bitcoins and Bank of America:

a. On November 5, 2013, there were two bitcoin sale transactions on Local Bitcoins for $350 and $340. That same day, there were two deposits into the Mediapen's Bank of America account for $350 and $340 with the description "counter credit."

b. On November 8, 2013, there were four bitcoin sale transactions on Local Bitcoins for $200, $350, $999.88, and $1,000. That same day, there were four deposits into the Mediapen's Bank of America account for $200, $350, $999.88, and $1,000 with the description "counter credit."

c. On November 9, 2013, there was a bitcoin sale transaction on Local Bitcoins for $378. On November 12, 2013, there was a deposit into the Mediapen's Bank of America account for $378 with the description "counter credit."

d. On November 12, 2013, there was a bitcoin sale transaction on Local Bitcoins for $801. That same day, there was a deposit into the Mediapen's Bank of America account for $801 with the description "counter credit."

26. In total, from November 2013 to October 2014, there were over $100,000 in cash deposits into Mediapen's Bank of America account, the majority having the description "counter credit."

27. Open source records indicate that RICHO currently may be living at an address in Wallingford, Connecticut. On September 26, 2016, I conducted surveillance of that address and observed a black Mercedes sedan with a Connecticut license plate parked on the street near the rear entrance to that address. According to records provided by the Connecticut Department of Motor Vehicles ("DMV"), the license plate on the car is registered to a Michael Richo having the same date of birth as the Michael RICHO who is the target of this investigation. The DMV records list the Wallingford address as RICHO's mailing address. Based on the foregoing information, I believe RICHO currently resides in Wallingford, Connecticut.

CONCLUSION

28. Based on the aforementioned information and statements, I believe there is probable cause that from approximately November 2013 to October 2014, the exact dates being unknown, in the District of Connecticut, RICHO committed access device fraud, in violation of 18 U.S.C. § 1029(a)(3) by possessing fifteen or more unauthorized access devices, namely usernames and passwords he stole from other individuals through an online phishing scheme, with intent to defraud. He also committed access device fraud, in violation of 18 U.S.C. § 1029(a)(2) by using one or more of those login credentials to steal more than $1,000 worth of bitcoins from those other individuals during that period.

29. Based on the aforementioned information and statements, I further believe there is probable cause that from approximately November 2013 to October 2014, the exact dates being unknown, in the District of Connecticut, RICHO committed computer fraud, in violation of 18

U.S.C. §§ 1030(a)(2) and (a)(4) by using stolen usernames and passwords to access the bitcoin accounts of other individuals to obtain more than $5,000 worth of bitcoins during that period.

30. Based on the aforementioned information and statements, I further believe there is probable cause that from approximately November 2013 to October 2014, the exact dates being unknown, in the District of Connecticut, RICHO committed wire fraud, in violation of 18 U.S.C. § 1343, by devising and executing a scheme to defraud other individuals and obtain their bitcoins through materially false representations, namely, using stolen usernames and passwords to login to their bitcoin accounts via the internet and then transferring the bitcoins to himself and selling the bitcoins for U.S. currency which was deposited into a bank account he controlled.

31. Based on the aforementioned information and statements, I further believe there is probable cause that from approximately November 2013 to October 2014, the exact dates being unknown, in the District of Connecticut, RICHO committed aggravated identity theft, in violation of 18 U.S.C. § 1028A, by committing access device fraud, computer fraud, and wire fraud, by using means of identification, that is login credentials, of other individuals.

32. Finally, based on the aforementioned information and statements, I believe there is probable cause that from approximately November 2013 to October 2014, the exact dates being unknown, in the District of Connecticut, RICHO committed money laundering, in violation of 18 U.S.C. § 1956(a)(1)(B)(i), by selling the bitcoins he obtained as a result of the aforementioned violations in exchange for U.S. currency and then causing the currency to be deposited into a bank account controlled by him in order to conceal or disguise the nature, location, source, ownership or control of such proceeds.

33. Therefore, I respectfully request that a criminal complaint be issued to support the arrest of and to charge RICHO with the TARGET OFFENSES.

REQUEST TO SEAL

34. Because this application pertains to an ongoing criminal investigation, and because disclosure of the information contained herein as well as disclosure of the arrest warrant and criminal complaint being requested herein may compromise the investigation, increase the risk of harm for the law enforcement officers responsible for executing the warrant, and result in the flight of the target of this investigation, the destruction of evidence, and the tampering with witnesses, I respectfully request that the criminal complaint and affidavit be ordered sealed until further order of the Court, except that copies may be provided to other law enforcements agents who are participating in this investigation, and copies may also be provided to counsel for RICHO following his arrest and prior to his initial appearance in court.

Special Agent Michael Morrison
Federal Bureau of Investigation

Subscribed and sworn to before me this 3rd day of October, 2016

/s/ Sarah A. L. Merriam
HON. SARAH A. L. MERRIAM
UNITED STATES MAGISTRATE JUDGE