SEALED BY ORDER OF COURT

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Northern District of California

FILED

09 2018

SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE

United States of America
v.
Jerry Ji Guo

Case No. CR 18 71598 MAG

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the fol1owing is true to the best of my knowledge and belief.

On or about the date(s) of August 2018 in the county of Santa Clara in the Northern District of *California*, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. s. 1343	Wire Fraud

This criminal complaint is based on these facts:

Please see attached affidavit of FBI Special Agent Mark R. Matulich.

Continued on the attached sheet.

Approved as to form · AUSA ____

Complainant's signature

FBI Special Agent Mark R. Matulich

Printed name and title

Sworn to before me and signed in my presence.

Date: 11/14/18

Judge's signature

City and state: San Jose, California

Hon. Susan van Keulen, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF A CRIMINAL COI\1PLAINT

I, Mark R. Matulich, a Special Agent of the Federal Bureau of Investigation ("FBI"), being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. This complaint is presented in support of an application for an arrest warrant for Jerry Ji Guo ("Guo").

2. As set forth herein, there is probable cause to believe that Guo has engaged in an ongoing scheme **to** defraud individuals residing in the Northern District of **California** and elsewhere pursuant to an ongoing wire fraud scheme in violation of Title 18, United States Code, Section 1343, Wire Fraud.

3. The contents of this affidavit are based upon the following: my own investigation; information obtained from other law enforcement agencies; my review of documents and computer records related to this investigation; oral and written communications with others who have personal knowledge of the events and circwnstances described herein; review of public information, including information available on the Internet; review of records received via legal process; and my experience and background as a Special Agent of the FBI. Statements made by witnesses and other individuals referenced in this affidavit have been paraphrased. Since this affidavit is being submitted for the limited purpose of securing a warrant and order, I have not included each and every fact lmown to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that violations of United States laws occurred.

4. I am an "investigative or law enforcement officer of the United States" within the meaning of Section 2510(7) of Title 18, United States Code, that is, and officer of the United

States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 2516.

5. I am a Special Agent ("SA") of the Federal Bureau of Investigation ("FBI") and have been so employed since July 2010. As part of my duties, I investigate offenses involving financial fraud schemes including embezzlement, high-yield investment fraud, securities fraud, and other schemes. I have experience investigating financial crimes and have received specialized training on the conduct of these investigations.

6. I am a certified public accountant. Prior t my employment as an FBI Special Agent, I worked in public accounting as an auditor, corporate internal audit, and was a corporate controller.

APPLICABLE LAW

7. Title 18, United States Code, Section 1343 provides whoever, 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, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both.

BITCOIN AND ETHER BACKGROUND

8. Bitcoin ("BTC") and ether ("ETH") are forms of decentralized, convertible, digital cryptocurrency that use online, decentralized ledger systems called blockchains, to store and transfer the currency. While BTC and ETH are mainly Internet-based forms of currency, it is possible to "print out" the necessary information and exchange BTC and ETH via physical medium. BTC and ETH are not issued by any government, bank, or company, but rather are

generated and controlled through computer software operating via the decentralized network. To acquire BTC and **ETH,** a typical user will purchase them from a BTC or ETH seller or "exchange." **It** is also possible for a user to "mine"{or earn) BTC and ETH by verifying other users' transactions. The computer time used in this verification process entitles the provider of that computer time to some pre-arranged amount of BTC or ETH. BTC and ETH are just two **forms** of digital cryptocurrency, and there are a significant number of other varieties.

9. Virtual currency exchanges typically accept payments of "fiat" currency (currency which derives its value from government regulation or law, such as US dollars), or other convertible digital currencies. When a user wishes to purchase BTC or ETH from an exchange, the user will typically send payment in the form of fiat currency, often via bank wire or ACH (Automated Clearing House) transactions, or other convertible digital currency to an exchange, for the corresponding quantity of BTC or ETH, based on a fluctuating exchange rate. The exchange will then typically attempt to broker the purchase with another user of the exchange that is trying to sell **BTC** or **ETH,** or, in some instances, will act as the seller itself. If the exchange can place a buyer with a seller, then the transaction can be completed. The exchange generally charges a commission for these services.

BTC AND ETH ADDRESSES

10. When a user acquires BTC or ETH, ownership of the BTC or ETH is transferred to the user's BTC or ETH address. The BTC and ETH addresses are somewhat analogous to bank account numbers, and are comprised of a case-sensitive string of letters and numbers amounting to a total of 26 to 35 characters for BTC and 42 characters including a "Ox" prefix for ETH. The user can then conduct transactions with other BTC or ETH users, by transferring BTC or ETH to their respective addresses, via the internet.

BTC AND ETH TRANSACTIONS AND THE BLOCKCHAIN

11. Little to no personally identifiable information about the payer or payee is transmitted in a BTC or ETH transaction. BTC and ETH transactions occur using a public key and a private key. A private key is an alphanumeric string kept secret by users and designed to sign a digital communication when used along with a public key. A public key is used to receive BTC and ETH, and a private key is used to allow withdrawals from a BTC or ETH address. Only the BTC and ETH address of the receiving party and the sender's private key are needed to complete the transaction. These two keys by themselves rarely reflect any identifying information.

12. All BTC and ETH transactions are recorded on what is known as the blockchain. This is essentially a distributed public ledger that keeps track of all BTC and ETH transactions, incoming and outgoing, and that updates approximately six times per hour. The blockchain records every BTC and ETH address that has ever received a BTC or ETH and maintains records of every transaction for each BTC and ETH address. In some circumstances, using the blockchain, BTC and ETH payments may be traced to accounts at traditional financial institutions.

INITIAL COIN OFFERING

13. Initial Coin Offerings ("ICOs") are a relatively new way to fund start-ups and projects. Similar to an IPO, an ICO is a way for a start-up or an established company to raise capital, and a vehicle of investment for potential investors. Usually, capital and "shares" in cryptocurrency/blockchain start-ups and projects are represented in tokens. In an ICO, the companies seeking funding sell their cryptocurrency tokens in exchange for financial investment or other contributions; the funding is executed using BTC, ETH, or other cryptocurrencies.

14. The first step for projects and start-ups is to spread the word about the ICO to attract as many potential investors as *possible*. Usually, announcements are made on relevant cryptocurrency forums (Bitcointalk, Reddit, etc...). The announcement contains an executive sununary of the project goals and ambitions. Additional information, such as notable and unique features of the project as well as the acting team members and their previous experience and track record are helpful to attract potential investors.

15. Since the start-up conducting the ICO is usually not well known, the marketing campaign plays and important role in a successful ICO. Specialized agencies may be hired to present at various conferences, conduct road shows, etc. From the perspective of communicating the project goals, it is important to have a white paper that clearly outlines the technical aspects of the product, the problems it intends to solve, and how it is going to solve them prepared before the launch of an ICO. A white paper usually accompanies an ICO for evidence purposes and outlines the content of the ICO, like a prospectus for an IPO, but with the key difference that white papers are not mandatory documents.

RELEVANT ENTITIES

16. BitGo: A blockchain security platform for virtual currencies, including BTC and ETH, based in Palo Alto, California. BitGo provides additional security for a BTC or ETH wallet by issuing three keys for each wallet. A private key is given to the customer, and a public key is held by BitGo. The third key is a backup private key, which is typically held offline in "cold storage" by a third party as a backup at the customer's discretion (hereinafter "backup **key'').** Cold storage refers to the method of storing digital information that is not connected to a web server or any other computer. Two of the three keys are necessary to transfer BTC or ETH to another address.

17. Gemini: a cryptocurrency exchange based in New York, New York, that allows customers to exchange virtual currency for fiat currency, or virtual currency for virtual currency, and its custody services provides segregated and omnibus custody services of virtual currency for its customers (collectively, the "Services"). Gemini allows customers to place various order types including "limit" orders to buy or sell virtual currency at specified prices on a spot exchange basis.

OVERVIEW OF SCHEME TO DEFRAUD

18. JERRY JI GUO ("GUO") orchestrated a scheme to obtain cash and cryptocurrency, specifically BTC and ETH, in the form of up-front fees and/or retainers for his services as an ICO consultant. GUO enticed prospective clients to enter into contracts with him by intentionally making materially false and misleading statements about his experience and credentials as an ICO consultant. Further, GUO misrepresented the nature and security measures of the multi-signature cryptocurrency wallets he directed his clients to transfer cryptocurrency to. Once GUO received up-front payments from his clients, he did little to no work as promised under the contracts. GUO directed cash to be transferred to a personal checking account at Bank of America ("BofA") ending in 0252, which was in the name of GUO and his mother. GUO transferred cryptocurrency held in what his clients believed were cryptocurrency wallets that were "escrow" in nature without the knowledge or permission of his clients to an account in his name at the Gemini cryptocurrency exchange which was tied to the same BofA checking account ending in 0252.

19. On August 20, 2018, security personnel at BitGo reported to law enforcement that they had received complaints from clients of GUO that cryptocurrency, namely BTC and ETH, had been transferred out of their accounts without their knowledge and consent. GUO, operating

as pressICO, convinced clients to add wallets into his enterprise setup at BitGo. The victim clients stated that they had entered into consulting contracts with GUO and transferred BTC and ETH to BitGo wallets based upon GUO's representations that he would not be able to transfer the cryptocurrency without their knowledge and consent because of BitGo's multi-signature solution to ensure security of funds.

20. In fact, GUO transferred the cryptocurrency out of his clients' BitGo wallets to other wallets, including at Gemini, that his clients had no lrnowledge of, and without their lmowledge and consent.

FACTS ESTABLISHING PROBABLE CAUSE

21. Between August and November 2018, the FBI interviewed several clients of GUO, including E.Z., D.R., J.G., and M.L., who related the following, in substance and in part:

a. GUO operated under the company names pressICO LLC, which was registered in Puerto Rico, and Kepler Capital Partners LLC, whose registration location is unknown, to provide client services as an initial coin offering ("ICO") marketing and publicity agency, including advisory and consulting related to the listing of cryptocurrencies on various exchanges.

b. GUO claimed to have an extensive network of contacts within the cryptocurrency industry, including exchanges such as Bitfinex (a cryptocurrency exchange headquartered in Hong Kong), and Binance (a cryptocurrency exchange founded in China and now headquartered in Malta).

c. GUO claimed pressICO collectively raised $165 million across nine ICOs, including $100 million for Polymath in a token sale management proposal and on the pressICO website.

d. GUO claimed he oversaw Polym ath,s $100 million ICO in a wbitepaper for a company called [redacted] as well as on [redacted] s website.

e. GUO instructed clients to transfer cryptocurrency, specifically BTC and ETH, to cryptocurrency wallets created on the BitGo platform ("BitGo wallets") in exchange for the type of services noted in "a" and "b" above.

f. In at least one instance, GUO instructed a client to wire transfer cash directly to his personal Bank of America ("BofA") checking account number ending in 0252 in exchange for the type of services noted in "a,, and "b" above.

g. GUO represented to clients that the BitGo wallets were "escrow" in nature, and required multiple levels of approvals, including client approval, before any transfer of funds out of the BitGo wallets would be possible.

h. GUO provided little to none of the services promised to clients within the contract period.

1. GUO circumvented BitGo security protocols to transfer client funds out of the BitGo wallets without client lmowledge or approval.

22. Bitfinex provided information to the FBI that they had only minimal contact via e-mail with GUO from his ji.guo.yale@gmail.com e-mail account in December 2017 regarding "a client looking to unload 35,000 btc,U and again in June 2018 regarding, "a couple projects (rate3.network / penta.global) who are willing to pay full price for listings..." In all, Bitfinex provided eight total e-mails with GUO regarding the listing of clients. Of these, GUO had drafted three e-mails from June 17 to 20, 2018. Bitfinex expressed interest in learning more in e-mails to GUO dated July 23 and August 20, 2018, however there did not appear to be any additional e-mail correspondence from GUO to Bitfinex. Previously, on December 8, 2017,

GUO participated in a six e-mail exchange with Bitfinex on an unrelated matter to "unload" 35,000 BTC. Bitfinex stated it had no known relationship with GUO beyond the e-mails noted above. None of the clients represented by GUO were listed on the Bitfinex exchange.

23. In response to an inquiry from the FBI, Binance stated that they were "unable to locate any relevant data" regarding GUO or the victim clients.

24. C.H., the co-founder of Polymath, told the FBI that GUO worked as a contractor to lead Polymath's marketing initiatives including on social media platforms such as Facebook. C.H. also told the FBI that Polymath ended its relationship with GUO after about a month and a halfbecause GUO did not actually do anything. Moreover, C.H. relayed that GUO worked with pressICO to generate what they believed were fake Facebook likes for Polymath, thus defrauding Pol a out of approximately $50,000 in up-front fees.- C.l1;. said any claims by GUO or pressICO that they were involved in raising $100 million for Polymath were completely false. Polymath attempted to contact GUO to ask him to remove any and all references to Polymath from the presslCO website, but GUO did not respond.

25. Representatives from three of the other ICOs GUO claimed to have raised funds for, i.e. Genesis Vision, BlockTix, and Viberate, also told the FBI they had not worked with GUO or pressICO.

26. The FBI interviewed the Chief Security Officer, the Chief Technology Officer, and others at BitGo who confirmed that GUO utilized two methods to circumvent BitGo security protocols, and transfer client funds out of the BitGo wallets without his clients' knowledge or authorization. First, GUO maintained control of the backup private keys for the BitGo wall ts. BitGo suggests and a typical setup is to place the backup private key in cold storage with a key recovery service because the backup private key can be used to transfer funds from BitGo

wallets without going through BitGo, or any security measures established within the BitGo wallets. GUO was fully aware of how the backup private keys worked, and knew if he retained control of those keys it gave him the ability to execute transactions with two keys - i.e. the backup private key and the known private key assigned to him - thus removing the need for the BitGo key and any security measures he led his clients to believe were in place that would require their involvement in any transfer of funds from their respective wallets.

27. Second, GUO set up "whitelisted" addresses belonging to him in the BitGo system. Whitelisted addresses were recognized as pre-approved to receive transfers of funds out of the BitGo wallets. These whitelisted addresses allowed GUO to transfer funds from his clients' BitGo wallets to his whitelisted addresses at any time without the need for any approval from his clients, thus circumventing the security protocols GUO's clients believed were required to effectuate a transfer of funds from their respective wallets including notification to them that a transfer had been requested and the need for their approval of that transaction.

28. As previously noted, two of three keys were required to transfer funds from the BitGo wallets GUO set up for his clients. GUO led his client's to believe that these two keys were a key held by GUO and a key held by BitGo. The satisfaction of a set of security protocols including minimum threshold amount per transaction and approval by additional administrators built into each wallet initiated the use of the BitGo key. As such, GUO used the existence of the BitGo key to reassure his clients that they would have control over and the ability to authorize transactions out of their respective wallets. In reality, GUO lmew he could bypass the BitGo key altogether by using the backup private keys he maintained control over. Further, GUO established a list of whitelisted addresses on the ETH wallets knowing transfers to wbitelisted

addresses would not trigger any additional notifications to other administrators over those wallets.

29. On August 19, 2018, GUO contacted BitGo, using e-mail address ji.guo.yale@gmail.com, to initiate a support ticket in order to obtain access to make enteiprise level changes to the settings of the BitGo wallets holding ETH, without his clients' knowl dge or consent. At 23:10 UTC, GUO removed an enterprise level rule that blocked any transactions from the ETH wallets. Once GUO removed this rule, he was able to make transfers of the cryptocurrency to pre-established whitelisted addresses. Within approximately 27 minutes of making this change, GUO executed three transfers totaling 4,274.58 ETH valued at approximately $1,287,759.97 from his clients' BitGo wallets to an account in his name on the Gemini exchange (account number 392768) without his client's knowledge or authorization.

30. Also on August 19, 2018, utilizing the methods outlined above, GUO used backup private keys to execute five transfers totaling 350.94129125 BTC valued at approximately $2,276,117.48 from his clients' BitGo wallets to an account in his name on the Gemini exchange (account number 392768) without his clients' lmowledge or authorization.

31. The investigation revealed that GUO undertook these actions from Bucharest, Romania. The following is a list of the transfers GUO executed:

II

II

II

II

II

II

Wallet ID	Date	Time (UTC)	Coin	Amount
5b387cf39f077cad0708204b64feee20	08/19/2018	23:32:19	ETH	1,275.84
Sb4230a96f29439632b99afd54b8bf5e	08/19/2018	23:37:42	ETH	1,961.75
Sb387dd75dbl565b079f70ec6d168a43	08/19/2018	23:34:50	ETH	1,036.99
	Total ETH Gemini Account Number 392768			4,274.58
Sb45e45137619861077841 1d5aec9f3f	08/19/2018	23:57:04	BTC	14.924
5b209c657a5946de6f5cc976d5531c38	08/19/2018	23:59:44	BTC	144.1927083
Sb0f5427f577c4d6442d5ddaf1796881	08/19/2018	21:55:50	BTC	85.48468581
Sb0f534f540ddeaf2e157c02bee e82d7	08/19/2018	21:37:43	BTC	98.63604159
Sb064829f996ece70cdb77388ca73829	08/19/2018	23:59:44	BTC	7.70385555
	Total BTC Gemini Account Number 392768			350.94129125

32. Gemini provided information that GUO is the sole administrator for account number 392768 on the Gemini exchange, and Bank of America ("BofA") account ending in 0252 is the sole bank account associated with the accoW1t. BofA account number 0252 is GUO's personal checking account. One of GUO's clients stated he facilitated multiple wire transfers totaling $195,000 to BofA account nwnber 0252 per GUO's jnstructions in exchange for GUO's promise to provide services which were for the most part never provided (see item "d" above under client interviews).

33. The FBI has communicated with security personnel at BitGo who informed the FBI that, after receiving inquiries and complaints from GUO's clients, they located the transferred cryptocurrency at Gemini. BitGo also identified 2,724.770611 ETH in two wallets under GUO's enterprise setup on their own system, and communicated with one of GUO's victim clients who had administrator privileges over those wallets. With that client's permission, BitGo transferred the 2,724.770611 balance of the wallets to a cold storage wallet under BitGo's control in order to safeguard the ETH from additional unauthorized transfers by GUO. BitGo communicated with Gemini, and both companies froze the cryptocurrency related to GUO's

BitGo wallets awaiting further guidance from law enforcement. On September 20, 2018, the FBI seized the cryptocurrency frozen in account number 392768 on the Gemini exchange pursuant to a seizure warrant issued in the Southern District ofNew York. On October 25, 2018, the FBI seized the cryptocurrency frozen in the BitGo cold storage wallet pursuant to a seizure warrant issued in the Northern District of California.

34. Per www.coindesk.com, a leading digital media, events, and information services company for the crypto asset and blockchain technology community, the price of BTC and ETH on August 19, 2018 was $6,485.75 and $301.26 respectively. Using these prices, the virtual currency GUO transferred without the knowledge or consent of his clients utilizing one of the two methods noted above to circumvent security protocols established on the BitGo wallets amounted to approximately $3,563,877.45 USD (ETH= $1)87,759.97 USO and BTC = $2,276,117.48 USD). Likewise, the ETH BitGo transferred to a cold storage wallet in order to prevent additional unauthorized transfers by GUO amounted to approximately $820,864.39.

35. Based on the foregoing, my training and experience, and the training and experience of agents and investigators involved in this investigation, I believe that there is probable cause to believe that JERRY JI GUO is involved in the commission of wire fraud in violation of Title 18, United States Code, Section 1343. Accordingly, I respectfully request a warrant be issued for bis arrest.

II

II

II

II

II

COUNTS ONE- THREE: 18 U.S.C. § 1343 WIRE FRAUD:

Count	Date	Initated From	To	Description
ONE	08/19/2018	California	New York	Electronic transfer of 144.1927083 BTC from "penta btc" BitGo wallet to GUO's account at the Gemini exchange.
TWO	08/19/2018	California	New York	Electronic transfer of 85.48468581 BTC from "upbit btc" BitGo wallet to GUO's account at the Gemini exchange.
THREE	08/19/2018	California	New York	Electronic transfer of 98.63604159 BTC from "bitfinex btc" BitGo wallet to GUO's account at the Gemini exchange.

SEALING REQUEST

36. Because this investigation is continuing, disclosure of the arrest warrant, this affidavit, and/or attachments thereto will jeopardize the progress of the investigation. In addition, disclosure of the arrest warrant at this time would seriously jeopardize the investigation and would allow GUO to change patterns of behavior, notify other confederates, destroy

II

II

II

II

II

II

II

II

II

evidence, or flee or continue flight from prosecution. Accordingly, I request that the Court issue an order that the complaint, arrest warrant, this affidavit in support of application for complaint and arrest warrant, and all attachments thereto be filed under seal until further order of this Court.

MARK R. MATULICH
Special Agent
Federal Bureau of Investigation

Sworn to before me this 5 day of November 2018.

HONORABLE SUSAN VAN KEULEN
United States Magistrate Judge