UNITED STATES DISTRICT COURT

for the

Northern District of California

United States of America
v.
DOUGLAS JAE WOO KIM

Case No. 3-20-70923 MAG

Defendant(s)

CRIMINAL COMPLAINT

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

On or about the date(s) of June 27, 2019 in the county of San Francisco in the Northern District of California, the defendant(s) violated:

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

Maximum Penalties: 20 years' imprisonment
$250,000 fine or not more than the greater of twice the gross gain or twice the gross loss
3 years' supervised release
$100 special assessment

This criminal complaint is based on these facts:

Please see the attached affidavit of FBI Special Agent Jennifer C Barnard.

☑ Continued on the attached sheet.

/s/ via Telephone
Complainant's signature

Approved as to form Scott Joiner
AUSA Scott Joiner

Jennifer C. Barnard, Special Agent, FBI
Printed name and title

Attested to by the applicant by telephone in accordance with the requirements of Fed. R. Crim. P. 4.1.

Date: 7/9/20

Sallie Kim
Judge's signature

City and state: San Francisco, CA

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

AFFIDAVIT OF JENNIFER C. BARNARD
IN SUPPORT OF A CRIMINAL COMPLAINT

I, Jennifer C. Barnard, 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. I make this affidavit in support of an application for a criminal complaint against Douglas Jae Woo KIM ("KIM"). As set forth below, there is probable cause to believe KIM engaged in an ongoing scheme to defraud individuals and obtain money or property through false or fraudulent pretenses, representations, or promises and then transferred the money or property to online gambling sites pursuant to an ongoing wire fraud scheme in violation of Title 18, United States Code, Section 1343. Specifically, as set forth in detail below, KIM represented to friends and acquaintances he was a cryptocurrency trader requesting loans for business purposes or to trade cryptocurrency. On multiple occasions, after receiving money or cryptocurrency, KIM would transfer all or portion of the assets to online gambling sites operating outside the United States.
2. The contents of this affidavit are based upon the following: my own investigation; my review of documents and computer records related to this investigation; my conversations with other law enforcement personnel; oral and written communications with others who have personal knowledge of the events and circumstances 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.
3. Statements made by witnesses and other individuals referenced in this affidavit have been paraphrased. In addition, certain electronic communications referenced in this affidavit are described in excerpted or summary fashion. Since this affidavit is being submitted for the limited purpose of securing a Complaint, I have not included every fact known to me concerning this investigation. I have set forth only the facts I believe are necessary to establish probable cause for the requested Complaint.

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, an 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 of the FBI and have been so employed since October 2007. As part of my duties, I investigate offenses involving financial fraud schemes, including investment fraud, corporate fraud, bank fraud, money laundering, and other schemes. I have experience investigating financial related crimes and have received specialized training on the conduct of these investigations.

6. Prior to my employment as a FBI Special Agent, I was an accountant.

COUNT ONE

7. Beginning in or about October 2017, and continuing through an unknown date, but until at least as recently as in or about July 2019, in the Northern District of California and elsewhere, the defendant, KIM, did knowingly and with the intent to defraud participated in, devised, and intended to devise a scheme and artifice to defraud as to a material matter, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and by means of omission and concealment of material facts. On or about June 27, 2019, in the Northern District of California and elsewhere, for the purpose of executing the aforementioned scheme and artifice to defraud and attempting to do so, the defendant did knowingly transmit and/or cause to be transmitted in interstate and foreign commerce, by means of a wire communication, certain writings, signs, signals, pictures, and sounds, specifically, a wire transfer initiated in the Northern District of California from a Wells Fargo bank account, that was transmitted in interstate commerce, all in violation of Title 18, United States Code, Section 1343.

APPLICABLE LAW

8. 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.

BACKGROUND REGARDING CRYPTOCURRENCY

9. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency include Bitcoin "BTC" and Ether "ETH". Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange (i.e., online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.[1] Cryptocurrency is not illegal in the United States.

10. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a

[1] Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key.") A public address is represented as a case-sensitive string of letters and numbers, 26–35 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key - the cryptographic equivalent of a password or PIN - needed to access the address. Only the holder of an address' private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

11. Bitcoin is a type of cryptocurrency. Mining is the way new Bitcoin are produced and the way Bitcoin transactions are verified. Individuals or entities located throughout the world run special computer software to solve complex algorithms that validate groups of transactions in a particular cryptocurrency. Under the Bitcoin protocol, which fosters a competition to verify transactions for inclusion on the public Bitcoin ledger, known as the "blockchain," the first miner to solve the algorithm is rewarded with a preset amount of newly issued Bitcoin.

FACTS ESTABLISHING PROBABLE CAUSE

12. The FBI interviewed multiple victims of KIM, to include VICTIM 1, VICTIM 2 and VICTIM 3, who relayed the following, in substance and in part:
    a. KIM represented himself as cryptocurrency trader;
    b. KIM requested loans for business purposes and/or to trade cryptocurrency;
    c. KIM was to repay the loans with interest;
    d. Assets in the form of cryptocurrency or U.S. currency were loaned to KIM based on these representations; and
    e. The victims would not have made the loans if the assets were to be used for gambling purposes, as opposed to what was represented.
13. According to the investigation, KIM used his scheme to obtain more than $4.5 million

dollars' worth of assets from the victims.[2]

A. VICTIMS 1 AND 2

14. On or about October 22, 2017, KIM contacted VICTIM 1 by way of text message. KIM introduced himself to VICTIM 1 and said he was looking for BTC investors interested in making what KIM called a short term loan for a "fairly modest operation where we are making a profit between peer to peer network and exchanges transaction fees."

15. On or about October 23, 2017, KIM texted VICTIM 1 and said he had approximately $300,000 to $400,000 in financial holdings and "The operation isn't very risky to me either so all around I don't feel worried about taking on the investment." KIM emailed VICTIM 1 the details of the loan; 10 BTC with an interest rate of 10% or 1 BTC to be repaid by December 15, 2017. KIM provided VICTIM 1 an address to receive the BTC. The email came from email address douglas.j.kim[XXXXX] (the last part of the email address has been obscured here for privacy purposes).

16. On or about October 24, 2017, VICTIM 1 sent approximately 10 BTC to the address provided by KIM. Per the website CoinMarketCap.com[3], on October 24, 2017, the price of BTC had a high of $5,935.52 and a low of $5,504.18.

17. On or about October 27, 2017, approximately 5 of the approximately 10 BTC was transferred to Nitrogen Sports, a cryptocurrency gambling site outside the United States. Nitrogen Sports purported to be the largest and most trusted bitcoin sportsbook and casino.

18. On or about December 31, 2017, VICTIM 1 introduced KIM to VICTIM 2.

19. VICTIM 2 and KIM signed a loan agreement dated January 1, 2018. The loan agreement was for 270 ETH with a fixed interest rate of 17% payable on or before March 1, 2018. The loan agreement included a continuation option and a personal guarantee. The address associated

---

[2] Based on applicable exchange rates on the day of the transfers.

[3] CoinMarketCap provides current price, market capitalization and volume data for cryptocurrency, as well as, historical data and charts. According to its website, CoinMarketCap is the "world's most-referenced price-tracking website for cryptoassets".

with KIM, per the agreement, was in San Francisco, California.

20. On or about January 1, 2018, VICTIM 2 sent or directed to be sent approximately 270 ETH to KIM. Per the website CoinMarketCap.com, on January 1, 2018, the price of ETH had a high of $782.53 and a low of $742.00. The ETH was deposited into KIM's account at Bittrex[4], a cryptocurrency exchange headquartered in Seattle, Washington. On or about January 1, 2018, approximately 170 ETH was exchanged into approximately 9.56 BTC, and approximately 4.5 BTC was transferred from KIM's account at Bittrex to Nitrogen Sports.
21. On or about January 6, 2018, an additional approximately 5 BTC was transferred to Nitrogen Sports.
22. On or about January 16, 2018, VICTIM 2 sent or directed to be sent approximately 270 ETH to KIM. Per the website CoinMarketCap.com, on January 16, 2018, the price of ETH had a high of $1,292.63 and a low of $875.54. The ETH was deposited into KIM's Bittrex account. From approximately January 16, 2018 to approximately January 31, 2018, approximately 270 ETH was exchanged into BTC and transferred from KIM's account at Bittrex to Nitrogen Sports.
23. For the most part, a similar pattern continued throughout VICTIM 1 and VICTIM 2's relationship with KIM. VICTIM 1 and VICTIM 2 loaned cryptocurrency to KIM. All or part of the cryptocurrency loaned was transferred to cryptocurrency gambling sites. I have identified approximately 14 transfers to KIM from VICTIM 1 in 2018-2019. For VICTIM 2, I have identified more than 10 transfers to KIM in 2017-2019.
24. VICTIM 2's last loan to KIM was on or about July 12, 2019. On or about July 11, 2019, VICTIM 2 agreed to loan KIM an additional 1,000 ETH with the understanding KIM would return the 1,000 ETH on or about July 14, 2019, and the interest earned shortly thereafter.
25. On or about July 12, 2019, VICTIM 2 sent or directed to be sent approximately 1,000 ETH to

[4] The account belonged to username douglas.j.kim[XXXXX] which matched an email address utilized by KIM. Bittrex was provided an image of KIM's Driver License.

KIM. Per the website CoinMarketCap.com, on July 12, 2019, the price of ETH had a high of $278.86 and a low of $268.00. The ETH was deposited into KIM's account at Kraken[5], a cryptocurrency exchange founded in San Francisco, California. On or about July 12, 2019, approximately 1,000 ETH was exchanged into BTC and transferred from KIM's account at Kraken to Fairlay[6], a cryptocurrency gambling site outside the United States. After the transfer, the remaining balance in KIM's Kraken account was approximately 0.004 BTC.

26. On or about July 13, 2019, VICTIM 2 texted KIM and asked KIM how the trading was going and if the extra leverage had been helpful. KIM responded it was "Definitely helpful" and he wanted more movement.

27. On or about July 14, 2019, the date KIM agreed to return VICTIM 2's 1,000 ETH, KIM texted VICTIM 2 and asked for an additional 12 to 24 hours so he could "see one more night and the Monday open + wires."

28. On or about July 17, 2019, KIM texted VICTIM 2 and said he did not "have any exchanges that work for me right this instant because of the withdrawal issue going on w Kraken."

29. From on or about July 15, 2019 until on or about July 17, 2019, three deposits and four withdrawals were made from KIM's Kraken account.

30. Between on or about October 24, 2017 and on or about July 12, 2019, VICTIM 1, himself/herself and on behalf of others, VICTIM 2, and an associate of VICTIM 2's, loaned KIM approximately 123 BTC, of which approximately 91 BTC remained outstanding, and approximately 15,252 ETH, all of which remained outstanding.

31. When interviewed by the FBI, VICTIM 1 and VICTIM 2 stated they would not have loaned money to KIM if they knew KIM was going to use it for gambling purposes.

---

[5] The name associated with the account was Douglas Jae Woo KIM and the address associated with the account was an address in San Francisco, California. Kraken was provided an image of KIM's Driver License, and a photograph including a handwritten note stating, "Only for trading digital currency on www.kraken.com".

[6] According to its website, Fairlay LLC was incorporated in the Republic of Costa Rica and does not accept customers and blocks IP addresses from the United States.

B. VICTIM 3 AND ONGOING SCHEME TO DEFRAUD

32. On or about June 18, 2019, KIM texted VICTIM 3 and asked, "feel like being a liquidity provider to DK capital for 1 month 5%?". When VICTIM 3 asked what that entailed, KIM explained it was a one month loan on which KIM would pay 5%. KIM told VICTIM 3 he could guarantee a loan of up to $50,000.

33. On or about June 19, 2019, VICTIM 3 texted KIM inquiring about the risk he/she was taking on to which KIM responded, "No risk besides me dying" and "I will carry risk and guarantee out of my assets". KIM provided VICTIM 3 his banking information, which included an address for KIM in San Francisco, California.

34. On or about June 23, 2019, VICTIM 3 texted KIM and asked KIM if he wanted to meet for dinner. KIM responded he was in Asia for the week for his father's birthday.

35. On or about June 27, 2019, KIM texted VICTIM 3 to make sure VICTIM 3 had not sent the money yet and asked VICTIM 3 if he/she could send the money within the next hour. VICTIM 3 stated he/she had an online banking limit and would have to go to a local branch to send the money. VICTIM 3 inquired as to whether he/she was sending $20,000 or $30,000, to which KIM responded, "Yeah that would be huge, market is being very fruitful right now" and "Could do 30 up to you". VICTIM 3 texted KIM he/she sent the money. KIM stated he set his calendar for July 28th. July 28, 2019, was approximately one month from the date VICTIM 3 sent the money.

36. On or about June 27, 2019, VICTIM 3 went to a Wells Fargo Bank branch in San Francisco, California to initiate the wire transfer. VICTIM 3 wired $30,000 to the Bank of America account KIM provided. On June 27, 2019, KIM's bank account had a negative balance of $15.54.

37. VICTIM 3's funds were transferred by wire and processed through the Fedwire Funds Service. Based on my training and experience and from other cases familiar to me, I know Fedwire funds transfers involve an exchange of electronic communications between facilities in New Jersey and Texas.

38. On or about June 27, 2019, KIM's Bank of America account received two wires totaling $60,000. On or about June 27, 2019, $59,000 was transferred from KIM's bank account to KIM's account at Gemini[7], a cryptocurrency exchange headquartered in New York, New York. On June 27, 2019, KIM's Gemini account had a beginning balance in United States dollars of $0.00. On or about June 27, 2019, $59,000 was exchanged into BTC and transferred from KIM's account at Gemini to Fairlay. After the transfer, the remaining balance in KIM's Gemini account was approximately 0 BTC.
39. On or about February 7, 2020, VICTIM 3 texted KIM about the loan. VICTIM 3 followed up with another text on or about February 14, 2020 and February 15, 2020. On or about February 17, 2020, KIM responded he had a small health scare the previous week, had not had his phone for a couple weeks, had to catch up on a bunch of stuff, would update VICTIM 3 that week, had not forgotten about him/her, and "You know I've got you". KIM stated he might "have to go offline on phone again" and provided VICTIM 3 his email address, douglas.j.kim[XXXXX].
40. On or about February 22, 2020, KIM emailed VICTIM 3 from the douglas.j.kim[XXXXX] email address. KIM stated he was going to fulfill his promise and stand by his words. KIM requested VICTIM 3's banking information, which VICTIM 3 provided.
41. On or about March 13, 2020, KIM texted VICTIM 3 "Hey, I am sure it's apparent that I am dealing with some larger issues I can't get into yet / would prefer in person, but like I said it's been my priority for awhile to pay you. My lawyer is preparing a document so that you are taken care of and paid promptly."
42. Victim 3 inquired about an update on or about March 18, 2020 and April 22, 2020. After inquiring on or about May 7, 2020, KIM responded "Hey sorry for delay, I got into some bad investments last summer and that's led to disputes now/made it complicated for me to just

[7] The name associated with the account was Douglas Jae Woo KIM and the address associated with the account was an address in San Francisco, California. Gemini was provided an image of KIM's Driver License.

freely make payment." KIM went on to say the simplest and fastest way to get VICTIM 3 paid ahead of a resolution would be to ask his parents to advance the payment and effectively buy the debt from VICTIM 3. KIM stated VICTIM 3 would receive payment the following day or week "for real this time".

43. On or about, May 15, 2020, VICTIM 3 received a return of funds.

44. When interviewed by the FBI, VICTIM 3 stated he/she would not have loaned money to KIM, if he/she knew KIM were going to use it for gambling purposes.

45. On or about February 12, 2020, the FBI received information KIM was actively soliciting new loans.

CONCLUSION

46. Based on the foregoing, my training and experience, and the training and experience of agents and investigators involved in this investigation, I respectfully submit there is probable cause to believe Douglas Jae Woo KIM has committed and may be continuing to commit wire fraud in violation of Title 18, United States Code, Section 1343.

/s/ via telephone
JENNIFER BARNARD
Special Agent
Federal Bureau of Investigation

Sworn to before me over the telephone and signed by me pursuant to Fed.R.Crim.P 4.1 and 4(d) this 9th day of July, 2020.

Sallie Kim
HON. SALLIE KIM
United States Magistrate Judge