UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

United States of America,

Plaintiff,

Civil No. 25-cv-12945
Honorable Judge:
Magistrate Judge:

vs.

Various cryptocurrency seized from Binance user id 61886539 in the name of [Person A],

Defendants *in rem*.

COMPLAINT FOR FORFEITURE

NOW COMES Plaintiff, the United States of America, by and through Jerome F. Gorgon, Jr., United States Attorney for the Eastern District of Michigan, and Kelly Fasbinder and Jasmine Moore, Assistant United States Attorneys, and states upon information and belief as follows in support of this Complaint for Forfeiture:

JURISDICTION AND VENUE

1. This is an *in rem* civil forfeiture action pursuant to 18 U.S.C. § 981(a)(1)(A), 18 U.S.C. § 981(a)(1)(B)(ii), and 18 U.S.C. § 981(a)(1)(C), resulting from violations of 18 U.S.C. §§ 1343, 1956, and 1957, and the Emergency Decree on Digital Asset Businesses of 2018, B.E. 2561.

2. This Court has original jurisdiction of this civil action by virtue of 28 U.S.C. § 1345, because it has been commenced by the United States, and by virtue of 28 U.S.C. § 1355(a), because it is an action for the recovery and enforcement of a forfeiture under an Act of Congress.

3. Venue is proper before this Court under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the government's claims occurred in the Eastern District of Michigan.

4. Venue is also proper before this Court under 28 U.S.C. § 1395 because the action accrued in the Eastern District of Michigan.

DEFENDANTS *IN REM*

5. The defendants *in rem* comprise cryptocurrency seized from Binance user id 61886539 in the name of [Person A], including the following:

a. 976.70914188 Bitcoin (23-FBI-008935);

b. 19,824.58545630384279859 Binance Coin (23-FBI-008934);

c. 766.11964752 Litecoin (23-FBI-008937);

d. 64.320401718803377994 Ethereum Classic (23-FBI-008938);

e. 35,838,067.7674885 Dogecoin (23-FBI-008945);

f. 3,183.960946574581724691 Ethereum (23-FBI-008939);

g. 27,200.6032008 Quant (23-FBI-003654);

h. 35,352.67891696 Hashflow (23-FBI-008946);

i. 1,171,317.26433951 Sandbox (23-FBI-008948);

j. 1,340,654.76512899 Decentraland (23-FBI-008947);

k. 7,617,454.988405 Tether (23-FBI-008936);

l. 40,458,204.89562177 Gala V2 (23-FBI-008949); and

m. 3,202.37008604 Ethereum PoW (23-FBI-008941).

6. The Federal Bureau of Investigation ("FBI") seized the defendants *in rem* from a Binance account ending in x6539 (the "Subject Account"), pursuant to a seizure warrant issued by the Hon. Alexander F. MacKinnon, in the Central District of California, on December 15, 2022. The Subject Account is controlled by "Person A"[1].

7. The defendants *in rem* are held in the custody of the United States Marshals Service or the FBI, where they shall remain subject to this Court's jurisdiction pending the resolution of this action.

UNDERLYING CRIMINAL STATUTES

8. 18 U.S.C. § 1343 ("Wire Fraud") prohibits anyone from devising or intending to devise any scheme or artifice to defraud, or to obtain money or property by means of false or fraudulent pretenses, representations, or promises, to transmit or cause to be transmitted by means of wire, radio, or television communication in

[1] Before the filing of this complaint, Person A entered into an agreement with the United States disclaiming any interest in the defendants *in rem*.

interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice.

9. 18 U.S.C. § 1956(a)(1)(B)(i) makes it a federal offense for anyone, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, to conduct or attempt to conduct such a financial transaction which, in fact, involves the proceeds of specified unlawful activity, knowing that the transaction is designed in whole or in part to conceal or disguise the nature, location, source, ownership, or control of the proceeds.

10. 18 U.S.C. § 1957 makes it unlawful for any person to knowingly engage or attempt to engage in a monetary transaction in criminally derived property of a value greater than $10,000 if the property is, in fact, derived from specified unlawful activity.

11. Pursuant to the Emergency Decree on Digital Asset Businesses of 2018, B.E. 2561 ("B.E. 2561"), it is unlawful to operate a "digital asset business" without compliance with Thailand's Anti-Money Laundering Act and subsequent amendments (collectively, the "Act").

12. Pursuant to B.E. 2561, a digital asset business includes any "digital asset dealer," which is defined as a person who provides services or holds themself out to the public as available to provide services with respect to the trading or exchange of digital assets for its own account in the normal course of business.

13. The Act, as applied by B.E. 2561, requires that any digital asset business collect detailed records regarding customer identities and sources of funds, and report all exchange transactions greater than 2 million Thai Baht in value.

14. The Act also prohibits transactions in funds derived from certain other "predicate offenses," including, but not limited to, certain gambling offenses.[2]

15. Under the Act, any person who commits an offense of money laundering may be imprisoned for a term of one year to ten years or to a fine of 20,000 Tahi Baht to 200,000 Tahi Baht, or both.

STATUTORY BASIS FOR CIVIL FORFEITURE

16. 18 U.S.C. § 981(a)(1)(A) provides for civil forfeiture of any property, real or personal, involved in a transaction or attempted transaction in violation of 18 U.S.C. §§ 1956, 1957, or 1960, or any property traceable to such property.

17. 18 U.S.C. § 981(a)(1)(C) provides for civil forfeiture of any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of a specified unlawful activity, which includes violations of 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1956 (Money Laundering), and 18 U.S.C. § 1957 (Spending).

[2] Specifically, the predicate offenses include any offense relating to gambling under the law on gambling, limited to offenses relating to being an organizer of a gambling activity without permission and there are more than one hundred players or gamblers at one time, or the total amount of money involved exceeds ten million Baht.

18 U.S.C. § 981(a)(1)(B)(ii) provides for civil forfeiture of any property, real or personal, within the jurisdiction of the United States, constituting, derived from, or traceable to, any proceeds obtained directly or indirectly from an offense against a foreign nation, or any property used to facilitate such an offense, if the offense would be punishable within the jurisdiction of the foreign nation by death or imprisonment for a term exceeding 1 year.

FACTUAL BASIS IN SUPPORT OF FORFEITURE

I. Background

A. Virtual Currency

18. Virtual currency (also known as cryptocurrency or digital currency) is generally defined as an electronic-sourced unit of value that can be used as a substitute for fiat currency (i.e., currency created and regulated by a government). Virtual currencies exhibit properties similar to other currencies, but do not have a physical form, existing entirely on the internet. Virtual currency is not issued by any government or bank (in contrast with "fiat" or conventional currencies) and is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Virtual currency is legal in the United States and accepted for legitimate financial transactions. However, it is also used for conducting illegal transactions or for concealing or disguising the true nature, source, location, ownership or control of illegally obtained criminal proceeds.

19. A virtual-currency exchange (an "exchange") is a business that allows customers to trade virtual currencies for other virtual or fiat currencies. An exchange can be a brick-and-mortar business, or strictly an online business. Both brick-and-mortar and online exchanges accept a wide variety of virtual currencies, and exchange them for fiat and traditional payment methods, other virtual currencies, or transfers between virtual currency owners. Many exchanges are located outside the boundaries of the United States to avoid regulation and legal requirements. One of the largest and most popular exchanges is Binance.

20. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, linked using cryptography, containing an immutable and historical record of every transaction. The blockchain is a decentralized, distributed, and public digital ledger that is used to record transactions across many computers in a way that the record cannot be altered retroactively without additionally changing all successive blocks and the consent of the network. Blockchain is a method to record transactions that provides high security by design: transactions are verified with advanced cryptography and spread across many computers in a peer-to-peer network or distributed ledger. The blockchain can be updated multiple times per hour and record every virtual currency address that ever received that virtual currency. It also maintains records of every transaction and all the known balances for each virtual

currency address. There are different blockchains for different types of virtual currencies.

21. Tokens are a form of digital asset that function similar to a virtual currency. Tokens are generally created by an issuing company and then used like currency by and within companies including the issuer, but are generally distinct from other blockchain-based cryptocurrencies such as Bitcoin. Digital tokens are often issued by companies attempting to launch a new digital product or digital service, where investors purchase tokens for cash and expect that they will exchange these tokens at a later date for greater value if the issuer is successful. While tokens can be used as a limited form of payment, these tokens officially remain the property of the issuer, which often will maintain technical tools that can restrict such tokens from being transferred further. In this way, a token may be analogized to a voucher or I-O-U, in that they are not specifically a currency, but represent value and may be exchanged at that value. Many tokens can be bought and transferred within certain exchanges, such as Binance.

22. One popular and commonly used token is Tether ("USDT"), a token issued by Tether Limited. Tether is a decentralized, peer-to-peer form of virtual currency having no association with banks or governments. Users purchase USDT, which is stored in a user's digital or cryptocurrency wallet (a "wallet"). USDT is generally considered a "stablecoin," meaning that it is intended to closely

approximate the value of the U.S. Dollar and thus can act as a virtual currency store of value similar to the U.S. Dollar. For this reason, cryptocurrency traders, both legitimate and illegitimate, will often convert other digital currencies into USDT for temporary or long-term storage, as by design, USDT typically does not experience the dramatic swings in value seen in other digital currencies.

23. A wallet is identified by unique electronic addresses that essentially stores the access code that allows an individual to conduct transactions on the public ledger. To access a wallet on the public ledger, an individual must use a public address and a private address. The public address can be analogized to an account number while the private address is similar to a password used to access that account. Even though the public address of those engaging in virtual-currency transactions are recorded on the public ledger, the true identities of the individuals or entities behind the public address are not recorded. If a real individual or entity is linked to a public address, however, it may be possible to determine what transactions were conducted by that individual or entity. Therefore, digital transactions are often described as "pseudonymous," meaning they are partially anonymous. Most individuals are identified when they use a virtual-currency exchange to make a transaction between virtual currency and fiat currency, or through virtual-currency exchangers that voluntarily or through legal order, cooperate with law enforcement.

B. Pig-Butchering Frauds

24. The cryptocurrency seized in this matter is largely derived from an investment-fraud scam commonly referred to as "pig butchering," perpetrated on victims throughout the United States, including in the Eastern District of Michigan. Pig-butchering schemes typically begin when a scammer sends a victim a seemingly innocuous or misidentified message. From there, the scammer will attempt to establish a more personal relationship with the victim by using manipulative tactics like those used in online romance scams.

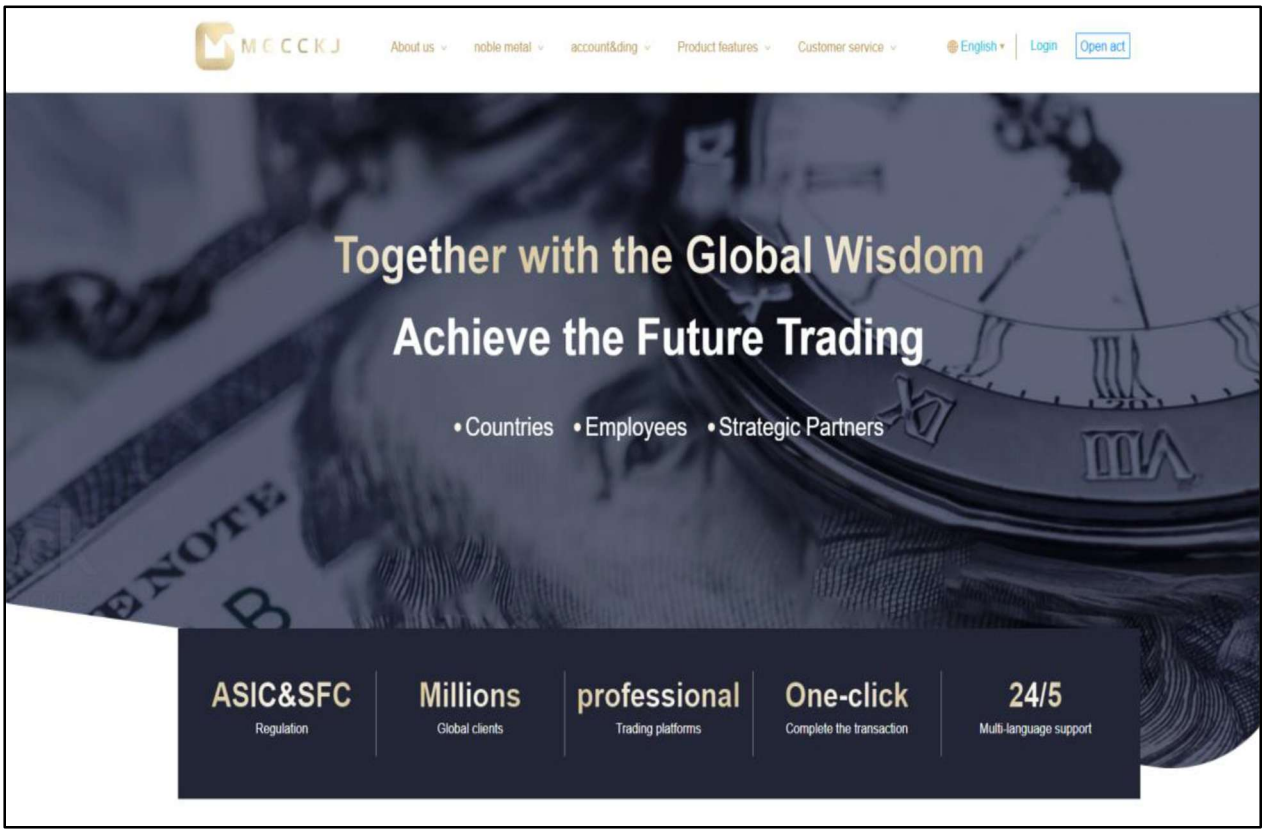
25. The victims in pig-butchering schemes are referred to as "pigs" by the scammers because the scammers use elaborate storylines to "fatten up" victims into believing they are in a romantic or otherwise close personal relationship. Once the victim places enough trust in the scammer, the scammer typically entices the victim into a cryptocurrency investment scheme. The investment schemes are fake but have the appearance of a legitimate enterprise through the use of fabricated interfaces, derivative or "spoofed" websites that appear related to legitimate companies, and other techniques designed to bolster the scheme's legitimacy. This generally includes a fake investment platform operated through a website or mobile application that displays a fictitious investment portfolio with abnormally large investment returns.

26. The investment platforms are a ruse, and the funds contributed are always routed to a cryptocurrency address the scammers control (this is when the scammers refer to "butchering" or "slaughtering" the victims). When the victims do attempt to withdraw their funds, they are unable to do so and are often met with various excuses or even required to pay "taxes" in order to release their funds. Eventually, most victims are completely locked out of their accounts and lose all their funds.

II. FBI Investigation

A. Overview

27. In this case, the FBI has identified victims with an estimated loss of at least $33.9 million related to these various fraudulent investment platforms, which sometimes appear to be offshoots of legitimate platforms. Some of the domain-name iterations identified include: www.deribit-e.com; www.deribit-x.com; www.deribit-exchange.net; www.deribitexin.site; www.mcus.me; www.toptankapp.com; and www.penzolead.com. Below is one example of a scam website, www.mgcckjs.com:



28. Many of the identified victims did not realize they were part of a scam until they attempted to withdraw some, or all, of their money. Some victims received excuses when attempting to withdraw their funds.

29. Based on review of financial documents and blockchain tracing, the FBI traced funds from the initial wallet addresses provided to the victims to the Subject Account. All dates are on or about the date specified and all amounts are approximate.

B. Victim J.Z. Loses $2.36 million in Investment Scam

30. Victim J.Z. was approached on Facebook by an unknown female using the name Jenny ("JENNY"). After a short conversation and after learning that J.Z. is retired, JENNY asked J.Z. to continue their conversations on the encrypted messaging service WhatsApp. JENNY presented herself as very successful, concentrating in real estate and financial investments. JENNY claimed to have a degree from the Wharton School of the University of Pennsylvania.

31. JENNY claimed to be an expert in gold spot trading. JENNY introduced J.Z. to a trading platform, MGCCKJ-FX, which she represented was a reputable company from Hong Kong. JENNY indicated to J.Z that her best friend was the CFO of the company. JENNY claimed to have $3 million in her account and sent J.Z. several screenshots of her trading with apparent large profits.

32. Based on these representations, JENNY convinced J.Z. to open a MGCCKJ-FX account with a minimal starting balance. J.Z. then traded under the guidance of JENNY, who convinced J.Z. to add more funds to the account. JENNY told J.Z. he could have financial freedom if he deposited more funds. MGCCKJ-FX also ran a purported promotion to encourage account holders to deposit more money by stating that if an account reached $1 million, the reward from the platform would be $199,999 plus a 60 percent discount on trading fees.

33. By early March 2022, J.Z. had deposited $1.1 million, and with his apparent trading gains, had an account balance of $2.4 million. JENNY continued to pressure J.Z. to deposit more money, setting a goal for him of $6 million. J.Z. refused to add more funds as he did not want to touch his retirement accounts, but JENNY responded to this by guiding J.Z. to make very aggressive trades, which J.Z. did.

34. The trades recommended by JENNY resulted in an apparent loss of J.Z.'s entire $2.4 million purported balance. JENNY apologized to J.Z. for the apparent loss and told him that if he could come up with $300,000, she would loan him $650,000 to make up for his losses. J.Z. then added additional funds, including an additional $100,000 from his retirement account. After several trades, J.Z.'s account appeared to be back up to $2.8 million. When J.Z. then refused to add more funds to his account, JENNY told J.Z. she wanted him to pay back the $650,000 she loaned him. J.Z. made a withdrawal request from MGCCKJ-FX, but the withdrawal request was denied, purportedly because the original loan from JENNY was now considered possible money laundering. The fraudulent platform requested evidence of the source of the $650,000 loan. JENNY refused to provide this information to the platform as it would expose her financial information.

35. J.Z.'s account was then purportedly frozen by MGCCKJ-FX, which stated that J.Z. needed to pay a verification fee of 16.5 percent of his account balance,

or approximately $466,000 to unfreeze his account. J.Z. made this payment out of his retirement account as he was afraid of losing access to his account. J.Z. was then required to pay an additional 7 percent of his account balance, or approximately $230,000, for "final" verification, and MGCCKJ-FX representatives told J.Z. he could withdraw all funds from his account after the fees were paid. If he did not pay the additional funds, he was told MGCCKJ-FX would again freeze his account. JENNY provided a screen shot to J.Z. with a guarantee from her best friend, purportedly the CFO of MGCCKJ-FX, that J.Z. would be able to withdraw all his money once final verification was made. J.Z. then paid the final verification fee.

36. Shortly thereafter, J.Z. attempted to withdraw $50,000 from his account. MGCCKJ-FX told him the withdrawal could not be made because of blockchain congestion, and he could not make the withdrawal unless he deposited $99,999 to be a VIP member of the platform. J.Z. made the additional deposit. J.Z. was then told his $50,000 withdrawal was successful but he never received the funds.

37. J.Z. attempted to contact MGCCKJ-FX but received no further communications. JENNY blocked J.Z. from her social media accounts and never talked to him again. J.Z. lost his entire investment of approximately $2.36 million.

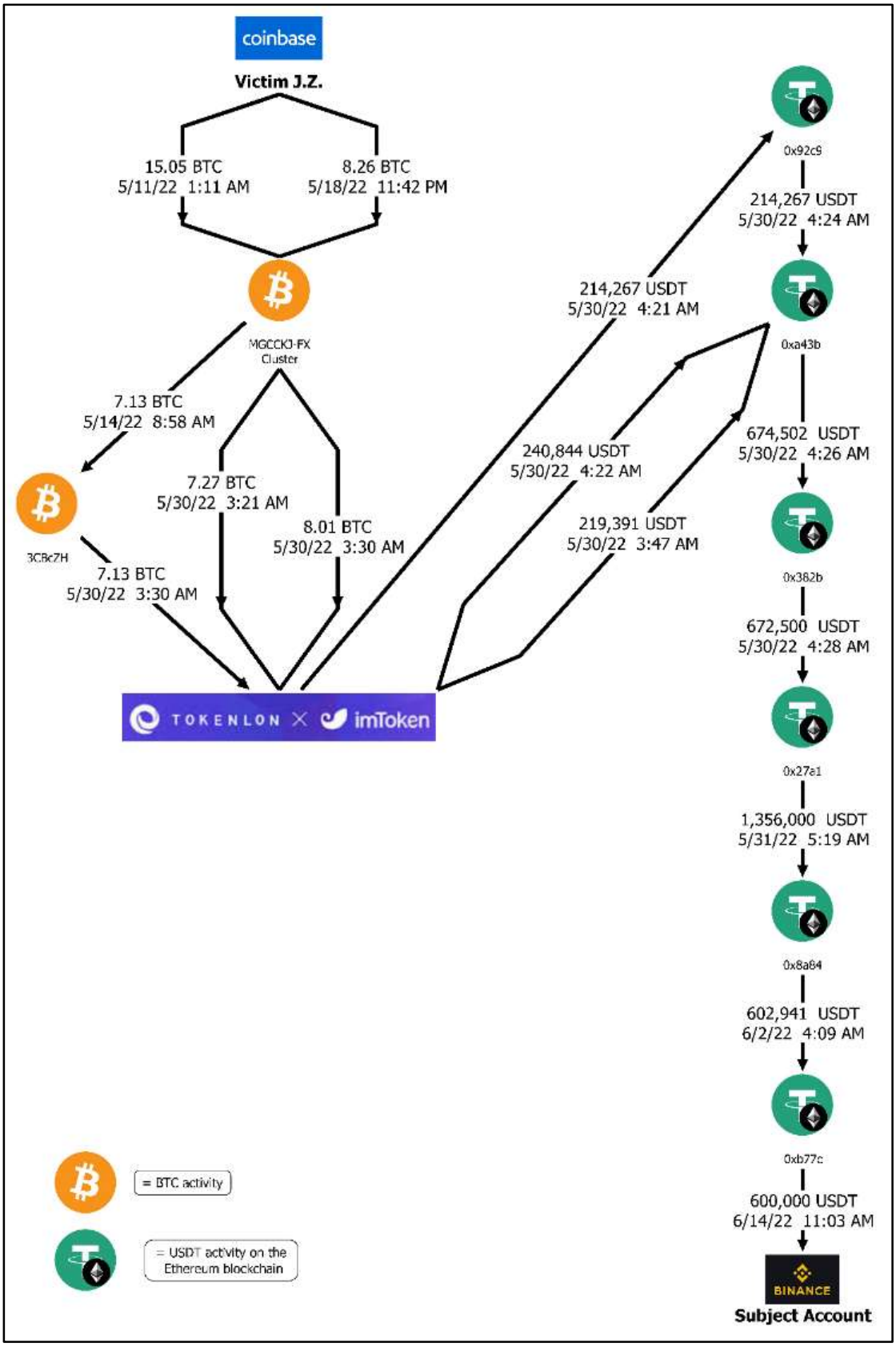
38. To make the purported investments described above, J.Z. sent bitcoin from his Coinbase account to a wallet address JENNY provided. On May 11, 2022, J.Z. sent 15.05 Bitcoin to a wallet address beginning with 35rxTq, at JENNY's

direction. In addition, on May 18, 2022, funds in J.Z.'s Coinbase account were converted into 8.26 Bitcoin and transferred to the same 35rxTq wallet address, also at JENNY's direction.

39. For purposes of blockchain analysis, 35rxTq is in a cluster of addresses herein referred to as the "MGCCKJ-FX Cluster." The MGCCKJ-FX Cluster also includes other Bitcoin addresses identified by the FBI as being highly likely under the control of the same owner based on change address analysis.[3]

40. J.Z.'s stolen funds were swapped from Bitcoin to USDT using the imToken and Tokenlon. The USDT was then consolidated into a wallet address beginning with 0xa43b and then rapidly transferred into and out of multiple intermediary wallet addresses, where the funds were commingled with other funds, before a portion of J.Z.'s funds arrived at the Subject Account. The below diagram summarizes the flow of funds from J.Z. to the Subject Account:

[3] Change-address analysis identifies addresses operating as change addresses for a particular wallet, where all addresses are controlled by the same owner. When an address spends Bitcoin, it must be spent in its entirety. Sometimes the value of the transaction is higher than what the owner wishes to pay, and in such a case, the wallet may generate a new Bitcoin address for which the owner also holds the private key and sends the difference back to this address. This is known as change. Change addresses are therefore highly likely held by the same owner as the original Bitcoin address.


coinbase
Victim J.Z.
15.05 BTC
5/11/22 1:11 AM
8.26 BTC
5/18/22 11:42 PM
MGCCKJ-FX
Cluster
7.13 BTC
5/14/22 8:58 AM
7.27 BTC
5/30/22 3:21 AM
8.01 BTC
5/30/22 3:30 AM
3CBkZH
7.13 BTC
5/30/22 3:30 AM
TOKENLON × imToken
214,267 USDT
5/30/22 4:21 AM
240,844 USDT
5/30/22 4:22 AM
219,391 USDT
5/30/22 3:47 AM
0x92c9
214,267 USDT
5/30/22 4:24 AM
0xa43b
674,502 USDT
5/30/22 4:26 AM
0x382b
672,500 USDT
5/30/22 4:28 AM
0x27a1
1,356,000 USDT
5/31/22 5:19 AM
0x8a84
602,941 USDT
6/2/22 4:09 AM
0xb77c
600,000 USDT
6/14/22 11:03 AM
BINANCE
Subject Account
= BTC activity
= USDT activity on the Ethereum blockchain

C. Victims L.Y., H.L., and A.C. Lose Millions in "Top Tank" Cryptocurrency-Investment Scams

a) Victim L.Y.

41. In March or April of 2022, victim L.Y. met a person on LinkedIn who went by the name of Bowen Chen ("CHEN"). L.Y. and CHEN began communicating and formed an online relationship that moved from LinkedIn to WhatsApp. CHEN presented himself as an architect who had his own firm.

42. During their communications, L.Y. began to trust CHEN and his advice. Soon, their conversations turned to cryptocurrency. L.Y. did not know anything about cryptocurrency or how it worked and trusted CHEN when he told her how to make money with it. L.Y. was open to learning something new and trusted CHEN and followed his advice.

43. CHEN told L.Y. that he had hired a group of analysts who were able to predict trade chances for higher returns. CHEN instructed L.Y. to start her cryptocurrency trading by downloading and creating an account with Coinbase. After she created an account with Coinbase, CHEN sent her a downloadable link for an application called "Top Tank." The Top Tank app she downloaded was the application she used to make her cryptocurrency trades at the advice and direction of CHEN.

44. During her trades, the fraudulent Top Tank app inaccurately showed L.Y. that she was profiting from her trades. L.Y. then tried to withdraw her funds from the Top Tank app to her Coinbase account. When she tried to withdraw her funds, she was told she had to pay a tax of $75,000 on her balance. L.Y. was in contact with Top Tank's purported Customer Service team via the Top Tank app to pay her taxes. L.Y. believed taxes were normal so she paid the $75,000 via cryptocurrency to Top Tank with the help of Top Tank's purported customer service guiding her through the process of payment.

45. Once she made the tax payment, she again tried to make a withdrawal of funds and was told her account credit was only at 75 percent, and it needed to be at 100 percent to make any withdrawals. L.Y. was told by purported customer service that in order to get her account credit up to 100 percent, she needed to pay more money. L.Y. was under the impression CHEN was also investing and had even invested more than she did and may have lost more than she did.

46. L.Y. no longer has contact with CHEN. L.Y. was never able to make any withdrawals from the Top Tank app and lost her entire investment of approximately $175,000.

47. As described further below in paragraphs 58-61, L.Y.'s funds were transferred and consolidated with other victim proceeds and then rapidly transferred

into and out of intermediary wallet addresses before a portion of the stolen funds were transferred to the Subject Account.

b) Victim H.L.

48. H.L. is the hiring manager for her company and uses LinkedIn. An unknown male going by the name Fei Kuang ("KUANG"), connected with H.L. on LinkedIn. KUANG sent his picture as well as a copy of his green card to H.L. KUANG claimed he used to work on Wall Street and was looking to start his own business. H.L. believed she was interviewing KUANG and asked him many questions.

49. KUANG started discussing cryptocurrency transactions with H.L., as she already had a Binance account with a balance of $4,000. KUANG told H.L. he was trading cryptocurrency and offered to teach her, and based on this representation, H.L. transferred additional funds into her account. KUANG then instructed H.L. to purchase additional cryptocurrency and transfer these funds to a BXMEX account. Eventually, KUANG told H.L. to move her funds from BXMEX to Top Tank due to purportedly lower fees at the latter platform. KUANG attempted to initiate a romantic relationship with H.L. but she thought it was inappropriate due to LinkedIn being a platform for business.

50. Upon attempting to withdraw funds from the fraudulent Top Tank, H.L. was told she had to pay taxes first. H.L. knew the United States would not require

taxes in that manner, so she researched the issue online. She found an article that the Chinese government required 20 percent taxes on any transaction, and H.L. then paid the required amount. After sending the money, a purported Top Tank representative told H.L. that her funds were involved in money laundering and insider trading. H.L. then realized she was the victim of a scam as the platform kept on trying to get her to pay more money without allowing her to withdraw any of her funds. Despite repeated attempts, H.L. never was able to make any withdrawals and lost approximately $2.5 million in the Top Tank platform scam.

51. As described further below in paragraphs 58-61, H.L.'s funds were transferred and consolidated together with other victim proceeds and then rapidly transferred into and out of intermediary wallet addresses before a portion of the stolen funds were transferred to the Subject Account.

c) Victim A.C.

52. In March 2022, A.C. was approached by someone going by the name Eden Lin ("LIN") on LinkedIn. LIN's profile stated he was a consultant at Crypto.com. A.C. and LIN became good friends and LIN purported to start teaching A.C. futures trading. LIN suggested they utilize a futures trading platform named "mcus.me," as he claimed to be familiar with the site. Over the next several months, LIN convinced A.C. to transfer all her previously owned cryptocurrency to

fraudulent platform mcus.me, as well as her liquidated retirement accounts and money from her regular bank accounts.

53. LIN convinced A.C. to withdraw the entire amount, totaling $2.9 million, to include apparent trading profits, from her mcus.me account. During the withdrawal process, A.C.'s mcus.me account was purportedly frozen, and mcus.me representatives stated that A.C.'s last transfer had a money-laundering issue, thus requiring a security deposit of $293,000 to facilitate the withdrawal. A.C. was able to raise $80,000 but not the entire $293,000. LIN told her he would help with the rest and instructed her to transfer the $80,000 to his private wallet. In June 2022, the mcus.me website disappeared.

54. In addition to the above mcus.me scam, A.C. was contacted in March 2022 by someone going by the name Zelin Wan ("ZELIN").

55. ZELIN claimed to be a University of Chicago alum and wanted advice on how to set up his new company. Zelin and A.C. started talking over the phone, and then via the messaging app LINE, and became friends. ZELIN wanted to show A.C. how he was trading cryptocurrency on a platform called Top Tank, and asked A.C. to transfer USDT to a newly created account. A.C. transferred $40,000 to ZELIN and he purported to showed her how to trade. The account quickly appeared to grow to approximately $60,000. When A.C. attempted to withdraw $30,000, her account was frozen purportedly because of money-laundering issues. Purported Top

Tank representatives then required A.C. deposit the equivalent amount of her entire account balance to unfreeze the account. ZELIN assured A.C. that he had withdrawn money from the platform before, so A.C. sent $50,000 to Top Tank with ZELIN telling her he would help with the additional $10,000.

56. Despite repeated attempts, A.C. was never able to make a withdrawal from either of the above-described fraudulent platforms. A.C. lost approximately $1.4 million in the mcus.me platform scam and approximately $100,000 in the Top Tank platform scam.

57. As described further below in paragraphs 58-61, A.C.'s funds were transferred and consolidated together with other victim proceeds and then rapidly transferred into and out of intermediary wallet addresses before a portion of the stolen funds were transferred to the Subject Account.

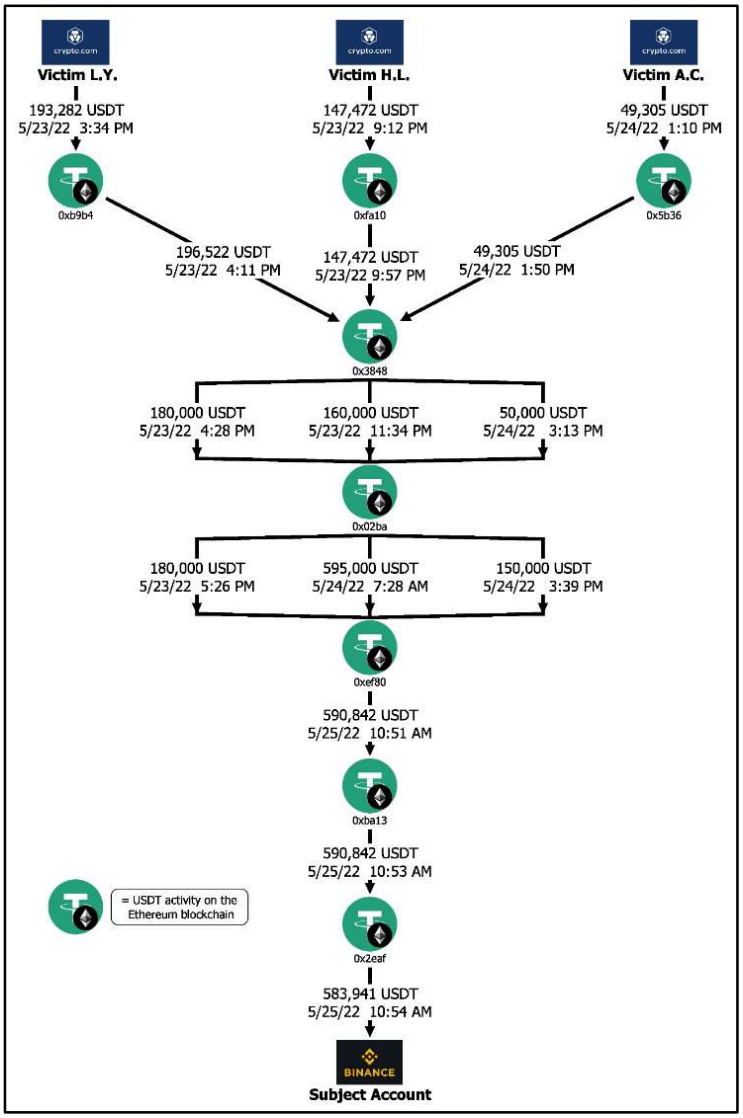
d) Funds from Victims L.Y., H.L., and A.C. Were Laundered to the Subject Account

58. On May 23, 2022, funds in L.Y.'s Crypto.com account were converted into 193,282 USDT and transferred to a wallet address beginning with 0xb9b4, at CHEN's direction.

59. On May 23, 2022, funds in H.L.'s Crypto.com account were converted into 147,472 USDT and transferred to a wallet address beginning with 0xfa10, at KUANG's direction.

60. A transfer also occurred on May 24, 2022, after funds in A.C.'s Crypto.com account were converted into 49,305 USDT and transferred to a wallet address beginning with 0x5b36, at ZELIN's direction.

61. L.Y.'s, H.L.'s, and A.C.'s stolen funds were transferred and consolidated in wallet address beginning with 0x3848 and then rapidly transferred into and out of multiple intermediary wallet addresses, where they were commingled with other funds, before a portion of the stolen funds arrived at the Subject Account:



D. Victims L.Z., Q.H., and D.C. Lose approximately $1 million in Deribit Cryptocurrency-Investment Scams

a) Victim L.Z.

62. In May 2022, a scammer contacted victim L.Z. and convinced L.Z. to invest in cryptocurrency using the website "deribit-e.net/wap/" (subsequently "deribit-i.xyz/wap/") and an associated application. The scammer told L.Z. the platform was a branch of Deribit.com and that the company was seeking approvals to operate in the United States.

63. L.Z. eventually invested approximately 239,715 USDT in his purported Deribit account. Over the following months, L.Z.'s account appeared to appreciate significantly, growing to approximately 5,211,000 USDT.

64. To realize the gain and pay expected U.S. taxes due in 2022, L.Z. attempted to withdraw his funds in July 2022. He requested two separate withdrawals of $50,000 and $100,000, respectively. The fraudulent platform, however, told him he could not make the withdrawals until he paid taxes of 3 percent of his profit, or approximately 150,000 USDT. Purported representatives of the platform said they would email him the form after L.Z. paid the required tax, and rejected L.Z.'s request to utilize his own deposited funds of approximately 239,715 USDT to pay the tax. The platform also refused to provide any tax reporting forms

for him to complete the transaction. L.Z. again tried to withdraw 180,000 USDT from his wallet and was blocked by the platform.

65. As described further below in paragraphs 79-82, L.Z.'s funds were transferred and consolidated together with other victim proceeds and then rapidly transferred into and out of intermediary wallet addresses before a portion of the stolen funds were transferred to the Subject Account.

b) Victim Q.H.

66. Q.H. was approached on LinkedIn by someone going by the name Boris Lin ("LIN"). After communicating on LinkedIn, they soon moved their communications to WhatsApp and LINE. LIN introduced Q.H. to investing in cryptocurrency on the Deribit platform.

67. LIN claimed she was working on a project team for Deribit and claimed to have a promising investment opportunity. LIN instructed Q.H. to open accounts at Crypto.com and Kraken. Q.H. was then instructed to wire funds from his bank account to the exchange accounts and convert the funds to USDT. Q.H. was then instructed to transfer those funds to what he thought was a legitimate Deribit platform. LIN would then instruct Q.H. on when to make trades.

68. Q.H. eventually wanted to withdraw some of his funds. First, a purported representative of Deribit stated that Q.H.'s account was suspected of illegal activity and required a purported "Account Guarantee" of $88,000 for review.

Once his account was cleared, a purported representative of Deribit told Q.H. the funds would be returned to his account. Then a representative of Deribit claimed that Q.H. owed $134,000 in taxes. After Q.H. made the tax payment, a representative of Deribit required Q.H. to pay a Credit Enhancement Guarantee of $55,000.

69. After making all the above requested payments, Q.H. attempted to make another withdrawal. Q.H. had done this numerous times by copying and pasting his wallet address to the request. On the latest withdrawal request, the last digit of his wallet address was somehow manipulated causing the withdrawal request to fail. A representative of Deribit insisted the wallet address was incorrectly entered by Q.H. The representative told Q.H. they recovered all his funds for him but now required Q.H. pay the equivalent of the total fund balance amount to successfully make the withdrawal.

70. Q.H. then realized he was the victim of a scam. Q.H. cut off contact with LIN after the representative of Deribit required him to pay all the extra fees. Q.H. was never able to make a withdrawal and lost his entire investment of approximately $337,500.

71. As described below in paragraphs 79-82, Q.H.'s funds were transferred and consolidated together with other victim proceeds and then rapidly transferred

into and out of intermediary wallet addresses before a portion of the stolen funds were transferred to the Subject Account.

c) Victim D.C.

72. Victim D.C. is a resident of Ypsilanti, Michigan and was proximally located there during at least some portion of the events described below.

73. D.C. was approached by an unknown person going by the name Anna on LinkedIn. D.C. later determined that this person also went by the name Lin Yu-Qing ("YU-QING"). YU-QING told D.C. that she lived in Canada, and after connecting on LinkedIn, YU-QING suggested they move their communications to LINE.

74. YU-QING told D.C. she was working for a tech company on a project in Toronto. She claimed she saw improper and large-volume trading in a cryptocurrency and told D.C. this was the opportunity of a lifetime. YU-QING instructed D.C. to download an application called Deribit and open an account to complete trades.

75. YU-QING first instructed D.C. to open accounts with Coinbase and Crypto.com, and D.C. was then told to wire transfer funds from his bank to these exchanges. YU-QING then instructed D.C. to transfer funds from his exchange account to an offshoot of Deribit.

76. YU-QING purported to show D.C. how to withdraw money from the platform as well. D.C.'s first withdrawal of $200 was successful, so D.C. thought the platform was legitimate. When D.C made trades that appeared to lose all his money, he then added more money to his account to try and make up what he believed he had lost. D.C. lost approximately $475,000 initially on the fraudulent platform.

77. YU-QING then told D.C. that she had made all her money back by borrowing from friends and relatives. D.C. received personal loans and invested again with the fraudulent platform. D.C.'s account then appeared to be as high as $615,900. He then tried to withdraw his money, but the fraudulent platform told him he could not withdraw any money as the system had frozen his account, purportedly because some of D.C.'s transactions may be illegal. To lift the freeze, D.C. was told he would have to pay 15 percent of his account for review, and if he did not pay, D.C.'s account would be terminated. A purported representee of the platform also told D.C. they would put him on the "black list" and report him to banks around the world. D.C. then contacted YU-QING, who told D.C. that this had happened to her as well, and that YU-QING's account was over $10 million, and she had to pay $1.8 million to unfreeze her account. YU-QING suggested that D.C. take out several personal loans to pay to unfreeze his account.

78. D.C. realized the platform and website were scams. D.C. eventually contacted the legitimate company Deribit, and a representative stated that they were going to open a case and conduct an investigation. D.C. lost his entire investment of approximately $500,000.

79. As described further below in paragraphs 79-82, D.C.'s funds were transferred and consolidated together with other victim proceeds and then rapidly transferred into and out of intermediary wallet addresses before a portion of the stolen funds were transferred to the Subject Account.

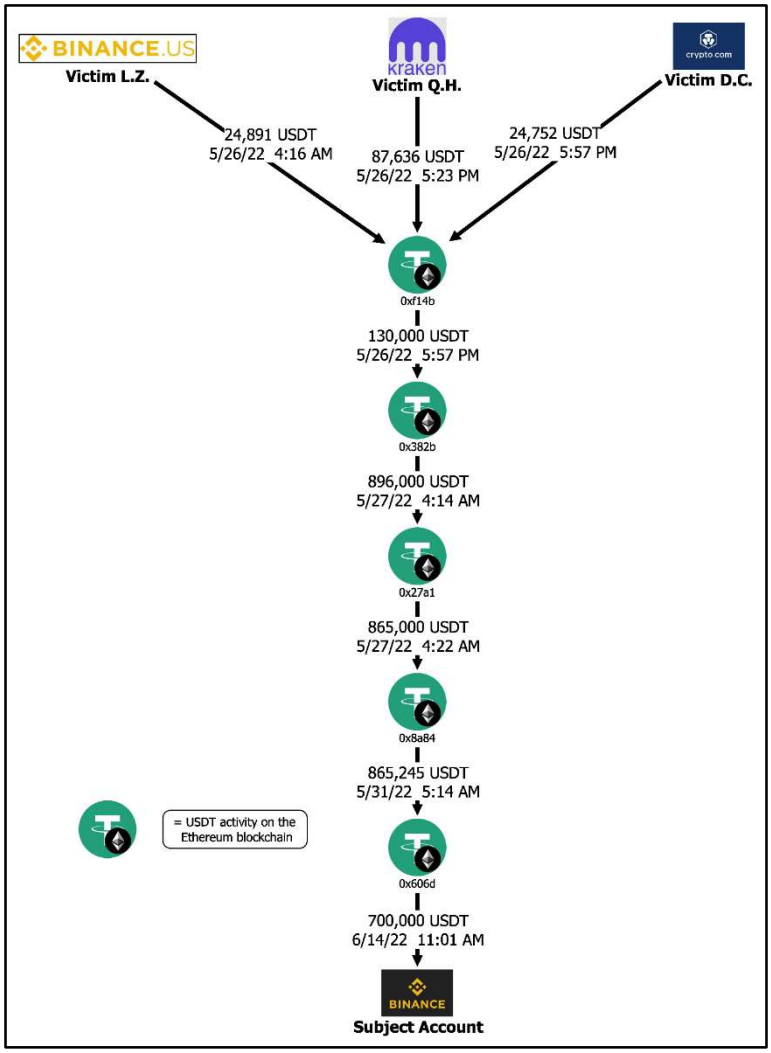
d) Funds from Victims L.Z., Q.H., and D.C. Were Laundered to the Subject Account

80. On May 26, 2022, funds in L.Z.'s Binance.US account were converted into 24,891 USDT and transferred to a wallet address beginning with 0xf14b, at LIU's direction.

81. On May 26, 2022, funds in Q.H.'s Kraken account were converted into 87,636 USDT and transferred to the same wallet address beginning with 0xf14b, at LIN's direction.

82. On May 26, 2022, funds in D.C.'s Crypto.com account were converted into 24,752 USDT and transferred to the same wallet address beginning with 0xf14b, at YU-QING's direction.

83. L.Z.'s, Q.H.'s, and D.C.'s stolen funds were consolidated together in the wallet address beginning with 0xf14b and then rapidly transferred into and out



of multiple intermediary wallet addresses, where they were commingled with other funds, before a portion of the stolen funds arrived at the Subject Account:

E. Victims K.F., M.T., and P.N. Lose Millions in Penzo and Sun Global Cryptocurrency Investment Scam

a) Victim K.F.

84. Victim K.F. was first contacted by a phone message from a person going by the name Jintong Guo ("GUO"). Shortly thereafter, they started to communicate via Skype, and GUO provided K.F. with a picture purportedly of herself.

85. GUO discussed investing in Bitcoin via a platform named Antrush. GUO instructed K.F. to wire funds from K.F.'s bank to Crypto.com. These funds were then transferred from Crypto.com to Antrush. In the beginning, K.F. only invested $20,000, but GUO showed K.F. how to make an apparent 30 percent return. Based on this representation, K.F. then invested substantially larger amounts—a total of $480,000 from his bank, $250,000 in personal loans, and approximately $100,000 from his 401(k) including an early withdrawal penalty.

86. In June 2022, purported representatives for Antrush told K.F. they were transferring his funds from Antrush to another platform named Penzo Limited ("Penzo"), with an address of www.penzolead.com/en/index. K.F. began to get nervous after the purported transfer to Penzo and tried to withdraw $440,000 of his money, but changed his mind and instead, successfully withdrew $200. A supposed Penzo representative told K.F. there was a trading event with a significant amount of funds to drag the market and K.F. could follow. The Penzo representative

instructed K.F. to follow the order. K.F. did as directed by the Penzo representative, and within minutes, all his funds appeared to be gone.

87. K.F. ultimately lost his entire investment of approximately $850,000.

88. As described further below in paragraphs 101-104, K.F.'s funds were transferred and consolidated together with other victim proceeds and then rapidly transferred into and out of intermediary wallet addresses before a portion of the stolen funds were transferred to the Subject Account.

b) Victim M.T.

89. Victim M.T. is a resident of Wales, Michigan and was proximally located there during at least some portion of the events described below.

90. Victim M.T. was contacted by text by an unknown person going by the name Ola ("OLA") and possibly named Xu Meina. OLA stated that she had texted M.T. by mistake as she was trying to get in touch with a client. OLA claimed to work for a clothing company in Laguna Beach, California. M.T. researched the company and the actual building. OLA and M.T. then moved their communications to WhatsApp.

91. M.T. ultimately believed that he was in a romantic relationship with OLA, who talked to him and sent him romantic songs, and promised to take him back to Hong Kong. OLA also spoke Cantonese, and sometimes M.T. would communicate with her using Google translate.

92. OLA talked to M.T. about cryptocurrency trading and convinced him to get involved. OLA admitted to M.T. that the cryptocurrency trading opportunity she was telling him about was purportedly based on insider trading. OLA did not want to get her broker in trouble. OLA told M.T. that he could make 90 percent profit in 120 seconds with the trading opportunities.

93. OLA instructed M.T. to open an account at Coinbase, and M.T. wired funds from his bank to this Coinbase account. OLA also instructed M.T. to use the Meta Trader 5 application for his cryptocurrency trades. From Coinbase, M.T.'s funds went to Anthereum, until OLA then told M.T. to stop sending funds there and instead instructed him to send funds to "trader.penzolead.com." Shortly thereafter, OLA instructed M.T. to send funds to "m.sunglobal.vip."

94. At this last platform, M.T.'s funds were purportedly frozen. In M.T.'s communications with purported Sun Global representatives, the company claimed to be based in the United Kingdom. When M.T. tried to withdraw funds to pay off some of the loans he took out as part of this cryptocurrency trading, purported Sun Global representatives told him that he could not withdraw his money without paying taxes first per the "IRS Blockchain Technology Cryptocurrency Authority," and that M.T.'s money would be released after he paid the purported tax. OLA urged M.T. to quit his job, liquidate his 401(k) and pay the purported $200,000 tax bill. M.T. refused and has not spoken to OLA since. M.T. subsequently contacted the

Internal Revenue Service and learned there is no "IRS Blockchain Technology Cryptocurrency Authority."

95. M.T. lost approximately $425,000 in the scheme.

96. As described further below in paragraphs 101-104, M.T.'s funds were transferred and consolidated together with other victim proceeds and then rapidly transferred into and out of intermediary wallet addresses before a portion of the stolen funds were transferred to the Subject Account.

c) Victim P.N.

97. Victim P.N. is a resident of Canton, Michigan and was proximally located there during at least some portion of the conduct described below.

98. Victim P.N. was contacted by an unknown female going by the name Susan, who told P.N. that her Chinese name was Huiming Chen ("CHEN"). CHEN texted P.N. and told him her mother told her to contact him for the possible purpose of marriage. P.N. told CHEN she had the wrong guy. CHEN apologized but kept in contact with P.N. Later, CHEN added P.N. to her friend group in the messaging application LINE.

99. CHEN told P.N. she lived in Orange County, California, and has her own custom clothing business. Soon after, CHEN told P.N. that she invests in cryptocurrency including Bitcoin and USDC, and that she was making good money

doing so. CHEN claimed she had an uncle that had a team doing investment analysis who would tell her when to make trades.

100. CHEN assisted P.N. with installing an application on his phone to open an account with Penzo. CHEN instructed P.N. to fund a Coinbase account with his money from his bank account. CHEN then told P.N. to purchase USDC, then transfer the USDC to his newly opened Penzo account. CHEN told P.N. not to trade on his own, but to wait for when she contacted him after she received tips from her uncle. CHEN proceeded to notify P.N. to make trades, and he followed her directions.

101. P.N. was apparently making approximately 20 percent on his investment, and after several successful trades, CHEN encouraged P.N. to invest more money and advised P.N. to take out personal loans that he could easily pay back after a few more trades. P.N. borrowed $280,000 and added approximately $400,000 of his own money to his Penzo account. Soon thereafter, his Penzo account had apparently doubled and was worth approximately $1.27 million.

102. In July 2022, CHEN instructed P.N. to make another trade similar to all the previously executed trades. In less than two minutes, all of P.N.'s funds were apparently gone, and P.N.'s Penzo account appeared to be down to zero. P.N. reached out to CHEN, but she disappeared and did not respond. P.N. tried reaching out to Penzo representatives but was unsuccessful.

103. As described further below in paragraphs 101-104, P.N.'s funds were transferred and consolidated together with other victim proceeds and then rapidly transferred into and out of intermediary wallet addresses before a portion of the stolen funds were transferred to the Subject Account.

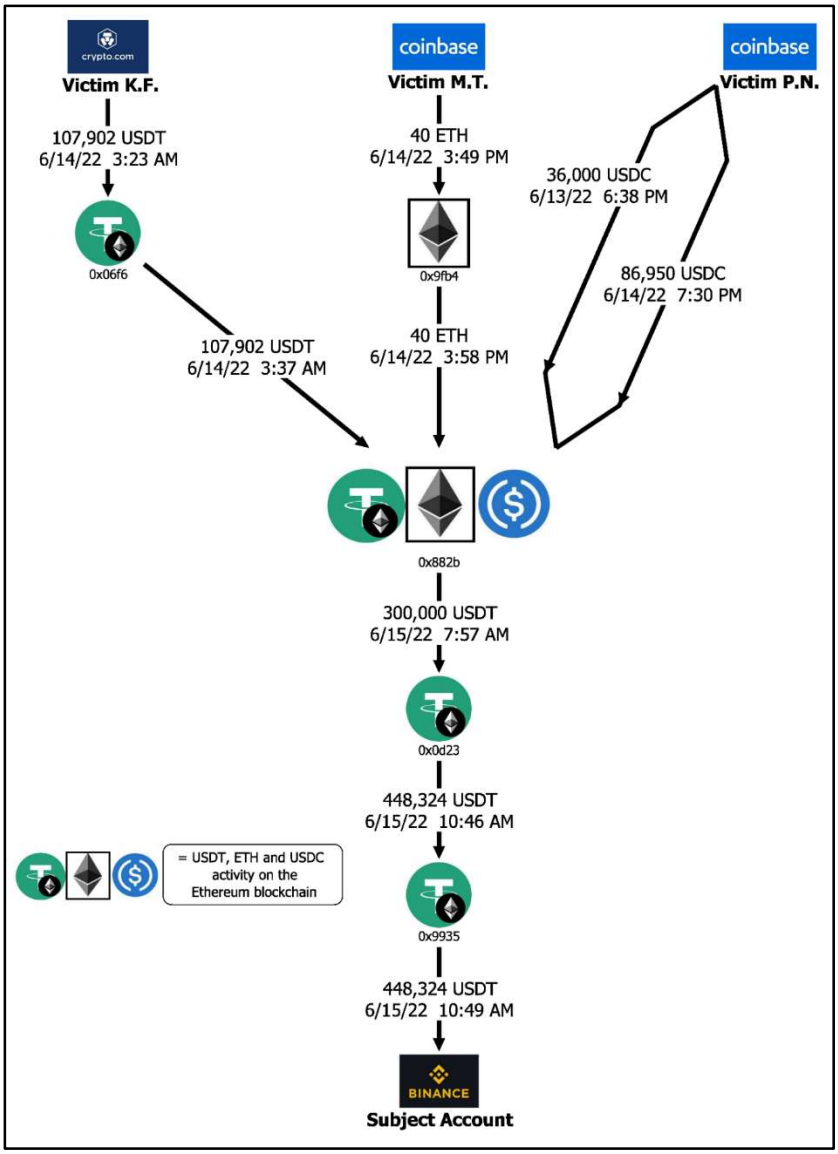
d) Funds from Victims K.F., M.T., and P.N. Were Laundered to the Subject Account

104. On June 14, 2022, funds in K.F.'s Crypto.com account were converted into 107,902 USDT and transferred to a wallet address beginning with 0x06f6, at GUO's direction.

105. On June 14, 2022, funds in M.T.'s Coinbase account were converted into 40 ETH and transferred to a wallet address beginning with 0x9fb4, at OLA's direction.

106. Two transfers also occurred, on June 13, 2022 and June 14, 2022, after funds in P.N.'s Coinbase account were converted into 36,000 USDC and 86,950 USDC and transferred to a wallet address starting with 0x882b, at CHEN's direction.

107. M.T.'s and P.N.'s stolen funds were swapped for USDT using Tokenlon. K.F.'s, M.T.'s, and P.N.'s stolen funds were then consolidated together in the wallet address starting with 0x882b and then rapidly transferred into and out of multiple intermediary wallet addresses, where they were commingled with other funds, before a portion of the stolen funds arrived at the Subject Account:

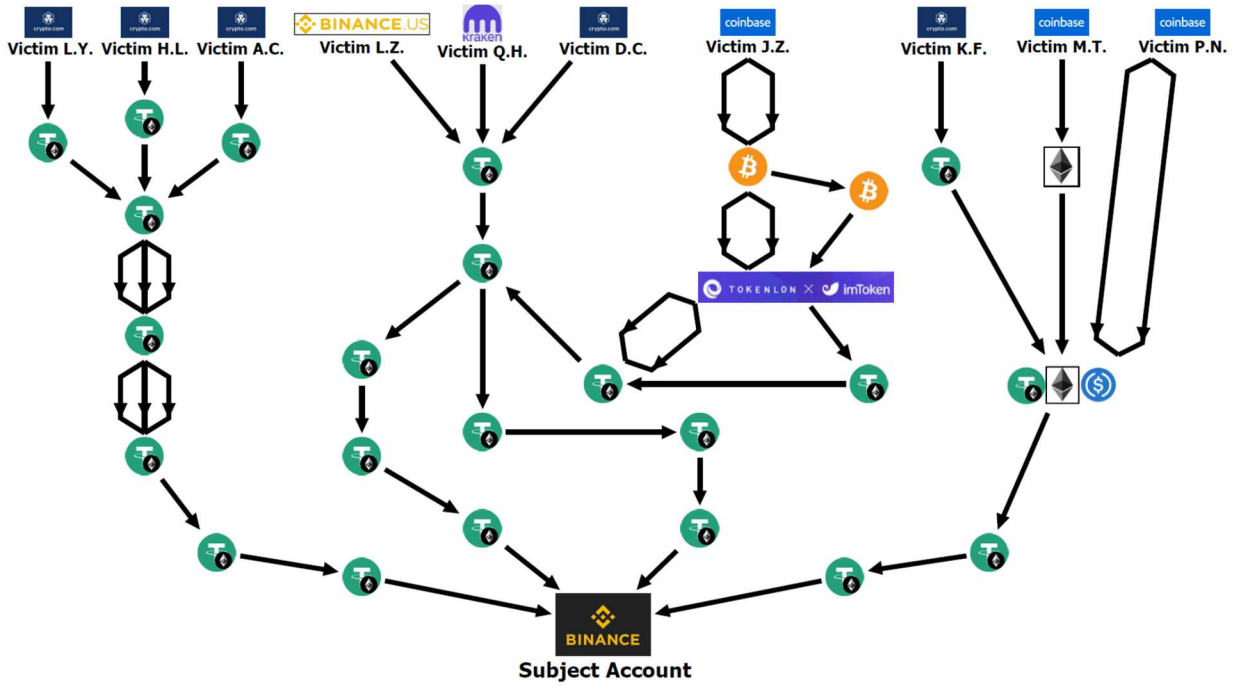


F. Tracing Victims Funds into the Subject Account.

108. In sum, each of the 10 victims above were victims of similar pig butchering schemes and all 10 of the victims had some portion of their "investments" directed to the Subject Account.

109. Even though each of the victims discussed above were targeted by different online personas, each had some of their stolen funds funneled to the Subject

Account. The following diagram depicts the sophisticated movement of victim funds described above, with the common denominator being that some portion of each victims' funds were directed to the Subject Account:



G. Person A Exchanges Cryptocurrency and Fiat Currency –and Executes Other Cryptocurrency-Related Transactions—for Profit on Behalf of Third Parties.

110. Person A resides and conducts business in Thailand.

111. In 2022, Person A was interviewed by the FBI in Thailand, and made the following admissions:

a. Person A's activities included spot and futures trading involving cryptocurrencies, as well as mining cryptocurrencies. Person A would buy and sell

cryptocurrencies for himself and on behalf of others. He would also exchange cryptocurrency for other types of cryptocurrencies or for cash on behalf of third parties, from which he would earn a profit.

b. Person A further stated that he had relationships with individuals who would transfer large quantities of USDT to Person A, via his virtual currency wallet in the Subject Account, and then Person A would deliver Thai Baht to these individuals at in-person meetings in Thailand.

c. Person A gambled at casinos and would fund accounts in casinos outside of Thailand with cryptocurrency. Certain cryptocurrency transactions between Person A and third parties were designed to provide access to USDT to finance activities at casinos.

d. Person A understood that at least one person with whom he transacted in cryptocurrency was operating as a middleman for others, and that the middleman received a 0.5 percent fee for this brokering service. Person A exchanged Thai Baht in person with the middleman, after which the USDT was transferred between Person A and the middleman.

e. Person A bought cryptocurrency from third parties who charged commissions from 0.5% to 1.5%, and Person A would sometimes pay the higher commissions to maintain the business relationship. In two to three years, Person A purchased tens of millions worth of USDT.

f. Person A admitted that the USDT he received for these exchanges often came from other wallets, which he then consolidated in the Subject Account.

g. After receiving USDT from an exchange, Person A would trade and invest the USDT he received, converting it into other virtual currencies and purchasing spot or options trades to increase the value of this virtual currency.

h. In other instances, anonymous individuals would want to buy USDT, which Person A would sell in return for fiat currency or other virtual currency.

H. Other Activity in the Subject Account is Consistent with Laundering Fraud Proceeds

112. From December 2020 to the date of seizure, approximately 208,000,000 USDT was deposited into the Subject Account.

113. Person A represented to Binance that the Subject Account was not a business account and was registered to him personally. However, Person A acknowledged to the FBI that he regularly bought and sold cryptocurrency as well as executed cryptocurrency-fiat exchanges on behalf of third parties for profit. On a daily basis, Person A would send third parties the price of USDT, after which the terms of a trade could be negotiated. Person A acknowledged that he often brokered cryptocurrency transactions among third parties. If the trade exceeded $3 million

Baht (which Person A understood to be Binance's daily limit), the transaction would be completed using cash Baht. Furthermore, Person A would lend USDT to third parties so that they could complete cryptocurrency trades.

114. The Subject Account was significantly funded with deposits of USDT consistent with the pattern described above (including multiple hops and short intervals of time between transactions).

115. In addition to the specific multiple victims' funds traced to the Subject Account as described above, further blockchain analysis of the Subject Account revealed what appears to be a sophisticated and deliberate effort to obfuscate the flow of funds into the Subject Account. The analysis demonstrates that an individual or group of individuals used multiple intermediary addresses and many Binance accounts to structure transactions to disguise the source of cryptocurrency received into the Subject Account.

116. As part of the investigation, the FBI obtained records for 24 Binance Accounts (hereafter referred to as "the 24 Binance Accounts") which were discovered by tracing cryptocurrency received into the Subject Account. Binance records demonstrate that the 24 Binance Accounts often shared account creation dates and were sometimes registered within minutes of each other. Each Binance account was opened using a unique name for which a Thailand identification document was provided for account confirmation. The 24 Binance Accounts are

each connected to Fiat currency Thai bank accounts, from which Thai Baht was transferred into the 24 Binance Accounts. The Thai Baht was subsequently used to purchase Tether (USDT) cryptocurrency, which is then withdrawn from the 24 Binance Accounts to specific cryptocurrency addresses on the Ethereum blockchain.

117. Based on further analysis, the FBI learned that the USDT withdrawals from the 24 Binance Accounts occurred numerous times on a daily basis, within close proximal time to each other, and were commonly in amounts of under 30,000 USDT (worth approximately $30,000 USD). This pattern of USDT withdrawals occurred over 3,600 times from April 2022 to October 2022, to the same five addresses on the Ethereum blockchain. In total, over 77 million USDT was withdrawn in this manner.

118. For example, the below diagram depicts 16 USDT withdrawals from 16 of the 24 Binance Accounts, all of which occurred on a single day. For each of the shown transactions, after the cryptocurrency was withdrawn from the Binance accounts, the USDT was transferred through multiple intermediary accounts before the USDT was deposited into the Subject Account.

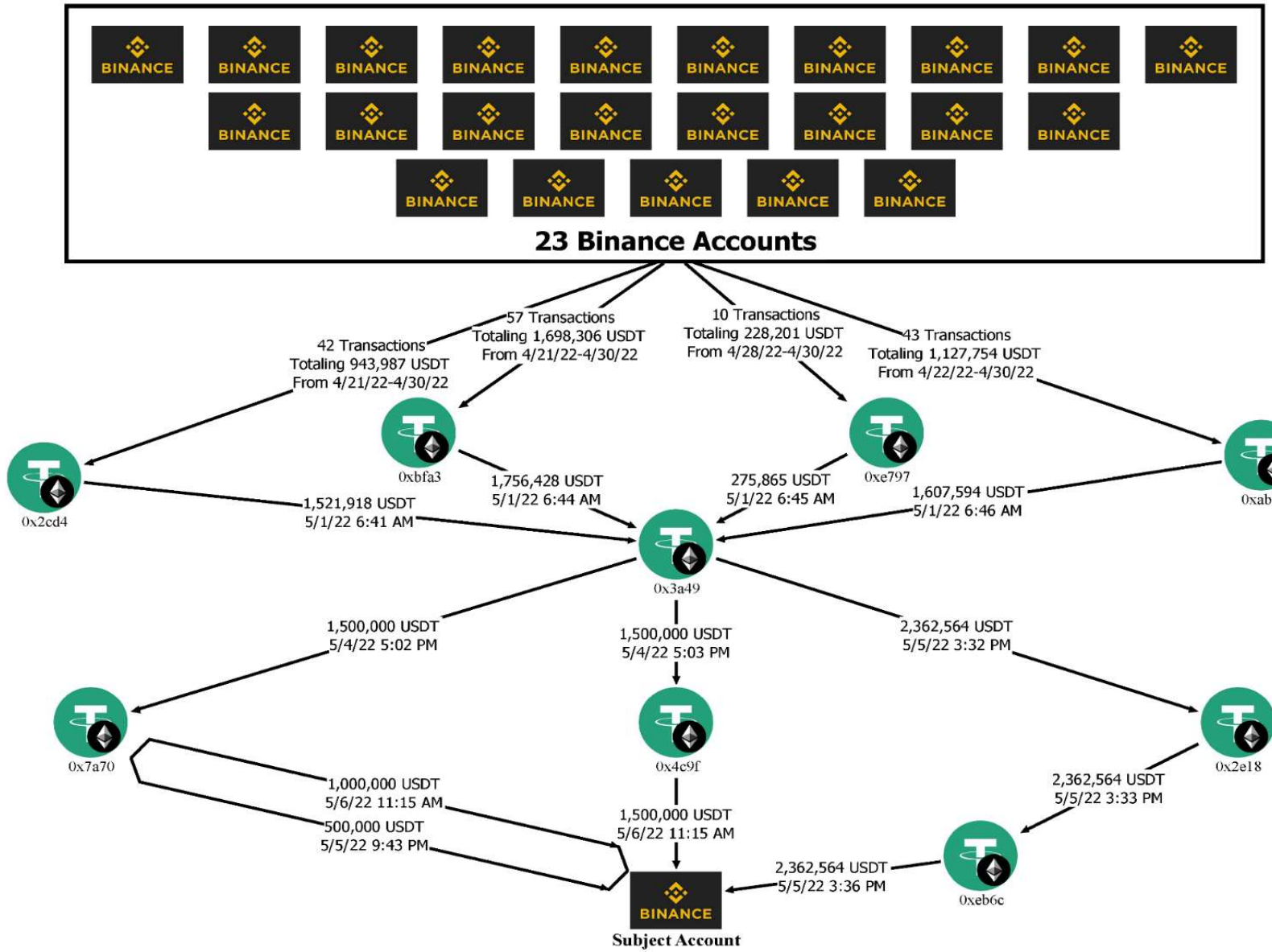
Date	USDT	From	To Receiving Address
4/23/2022 3:04	29,332.71	Binance Account 1	0xab0f
4/23/2022 3:58	29,332.70	Binance Account 4	0xab0f
4/23/2022 4:02	14,663.93	Binance Account 22	0xab0f
4/23/2022 4:23	2,926.85	Binance Account 18	0xab0f
4/23/2022 5:17	29,324.55	Binance Account 13	0x2cd4
4/23/2022 5:59	29,355.14	Binance Account 5	0xab0f

4/23/2022 6:04	29,393.10	Binance Account 7	0xbfa3
4/23/2022 7:12	14,685.52	Binance Account 2	0xab0f
4/23/2022 7:26	29,452.03	Binance Account 19	0x2cd4
4/23/2022 7:52	17,655.24	Binance Account 9	0x2cd4
4/23/2022 8:03	29,462.44	Binance Account 17	0xbfa3
4/23/2022 8:03	29,436.40	Binance Account 15	0x2cd4
4/23/2022 8:16	29,453.75	Binance Account 21	0xbfa3
4/23/2022 8:33	29,431.22	Binance Account 11	0xbfa3
4/23/2022 9:14	29,453.75	Binance Account 20	0xbfa3
4/23/2022 10:33	29,437.70	Binance Account 3	0xbfa3

119. As a part of a "layering" stage of the money-laundering process, criminals commingle fraud proceeds in consolidation wallets with other funds to conceal the nature, source, ownership, location, and/or control of the fraud proceeds—and, in that process, to make it harder for law enforcement to trace the disposition of the fraud proceeds. Here, the criminals appeared to commingle the fraud proceeds that they had obtained from various victims with the complex and structured flow of funds from the 24 Binance Accounts.

120. Due to the significant number of USDT withdrawals from the 24 Binance Accounts and the transfers between multiple intermediary addresses on the Ethereum blockchain, it is difficult for the FBI to analyze the over 77 million USDT that was withdrawn from the 24 Binance Accounts in its entirety. However, the FBI have identified multiple transactions of USDT moving from the 24 Binance Accounts that were ultimately funneled into the Subject Account. For each of these transactions, after the USDT was transferred through several intermediary addresses,

the USDT was deposited into the Subject Account from at least seven addresses on the Ethereum blockchain. In total, the Subject Account received over 55 million USDT from these transactions. Each of these transactions contained some amount USDT from the 24 Binance Accounts. For example, the below diagram shows an example of approximately 4 million USDT flowing out of the 23 of the 24 Binance Accounts, passing through intermediary addresses, and being deposited into the Subject Account from three of the seven addresses:


23 Binance Accounts
42 Transactions
Totaling 943,987 USDT
From 4/21/22-4/30/22
57 Transactions
Totaling 1,698,306 USDT
From 4/21/22-4/30/22
10 Transactions
Totaling 228,201 USDT
From 4/28/22-4/30/22
43 Transactions
Totaling 1,127,754 USDT
From 4/22/22-4/30/22
0x2cd4
0xbfa3
0xe797
0xab0f
1,521,918 USDT
5/1/22 6:41 AM
1,756,428 USDT
5/1/22 6:44 AM
275,865 USDT
5/1/22 6:45 AM
1,607,594 USDT
5/1/22 6:46 AM
0x3a49
1,500,000 USDT
5/4/22 5:02 PM
1,500,000 USDT
5/4/22 5:03 PM
2,362,564 USDT
5/5/22 3:32 PM
0x7a70
0x4c9f
0x2e18
1,000,000 USDT
5/6/22 11:15 AM
500,000 USDT
5/5/22 9:43 PM
1,500,000 USDT
5/6/22 11:15 AM
2,362,564 USDT
5/5/22 3:33 PM
2,362,564 USDT
5/5/22 3:36 PM
0xeb6c
Subject Account

121. Based upon my training and experience, there is no apparent reason, economic or otherwise, for the above described complex and structured flow of funds from the 24 Binance Accounts into the Subject Account. I therefore believe that the 24 Binance Accounts were established in coordination and are being utilized to conceal the nature, source, location, ownership and/or control of the funds at issue.

CLAIM FOR RELIEF

122. Based on the foregoing, the government alleges that the defendants *in rem* constitute property involved in transactions or attempted transactions in violation of 18 U.S.C. §§ 1956 & 1957 (relating to money laundering), and/or property traceable to such property, with the specified unlawful activity being violations of 18 U.S.C. § 1343. The defendants *in rem* are therefore subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A).

123. Based on the foregoing, the government alleges that the defendants *in rem* constitute property within the jurisdiction of the United States constituting, derived from, or traceable to, proceeds obtained directly or indirectly from an offense against a foreign nation, or property used to facilitate such an offense, with the specified unlawful activity being violations of the Act (as defined herein). The defendants *in rem* are therefore subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(B)(ii).

124. Based on the facts set out above, the government alleges that the defendants *in rem* constitute or are derived from proceeds traceable to violations of 18 U.S.C. § 1343 (wire fraud). The defendants in *rem* are therefore subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C).

CONCLUSION

WHEREFORE, Plaintiff, the United States of America, respectfully requests that this Court issue a warrant for arrest of the defendants *in rem*; that due notice be given to all interested parties to appear and show cause why forfeiture should not be decreed; that judgment be entered declaring the defendants *in rem* condemned and forfeited to the United States for disposition according to law; and that the United States be granted such other and further relief as this Court may deem just and proper, together with the costs and disbursements of this action.

Respectfully submitted,

JEROME F. GORGON, JR.
United States Attorney

/s/Kelly Fasbinder
Kelly Fasbinder (P80109)
Jasmine Moore (P82181)
Assistant United States Attorneys
211 W. Fort Street, Suite 2001
Detroit, MI 48226-3211
(313) 226-9520
Kelly.Fasbinder@usdoj.gov

Dated: September 17, 2025

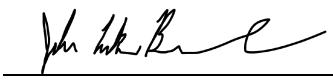
VERIFICATION

I, John Luke Bucuvalas, hereby declare that:

I am a Special Agent of the Federal Bureau of Investigation. I have read the foregoing Complaint for Forfeiture and declare under penalty of perjury that the facts contained therein are true to the best of my knowledge and belief, based upon knowledge possessed by me and/or on information received from other law enforcement agents and/or officers.

I declare under penalty of perjury that the foregoing is true and correct.

Executed September 15, 2025 in Phoenix, Arizona.



John Luke Bucuvalas
Special Agent
Federal Bureau of Investigation