AFFIDAVIT OF SPECIAL AGENT MICHAEL JANKOWIAK IN SUPPORT OF A COMPLAINT FOR CIVIL FORFEITURE

I, Special Agent Michael Jankowiak, state the following:

INTRODUCTION AND AGENT BACKGROUND

1. I have been a Special Agent for the Federal Bureau of Investigation ("FBI") since October of 2023. I graduated from the FBI Academy in Quantico, Virginia, where I received extensive training in conducting criminal investigations. I am assigned to FBI Boston's Financial Crimes Squad where I investigate complex financial crimes, including money laundering, wire fraud, mail fraud, and bank fraud, among others. Before becoming a Special Agent, I worked as an FBI Forensic Accountant and in public accounting as an auditor. I am a Certified Public Accountant ("CPA") and Certified Fraud Examiner ("CFE").

PURPOSE OF AFFIDAVIT

2. I submit this affidavit in support of a Verified Complaint for Forfeiture *in Rem* against the following USDT[1]:

a. approximately 1,283,763 USDT associated with the cryptocurrency wallet with address 0x617B4c0ef2388e7a893C8c47EB4b6D97a1657610 ("Target Wallet 1");

b. approximately 1,943,188 USDT associated with the cryptocurrency wallet with address 0xDF22A5C33944DAFa27D11799e62D8310b84BCcbA ("Target Wallet 2"); and

c. approximately 217,519 USDT associated with the cryptocurrency wallet with address TXufJnjkkGpQ3o7KvQndf2D2nUCFeWtaJr ("Target Wallet 3")

(collectively, the "Defendant Property").

[1] USDT is a stablecoin. Each USDT token is worth approximately $1.00 USD and claimed to be backed by $1.00 USD in physical reserves. Payments or transfers of value made with USDT are recorded in the blockchain network. Tether International S.A. de C.V. ("Tether") is the company that manages the smart contracts and the treasury (*i.e.*, the funds held in reserve) for USDT tokens.

3. As set forth below, there is probable cause to believe that the Defendant Property represents proceeds traceable to a violation of 18 U.S.C. § 1343 (wire fraud) and is property involved in violations of 18 U.S.C. § 1956 (money laundering) and is subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 981(a)(1)(C).

4. On February 20, 2025, the United States obtained a seizure warrant for 1,283,763 USDT stored in or accessible in Target Wallet 1 and 1,943,188 USDT stored in or accessible in Target Wallet 2. On March 12, 2025, the United States obtained a seizure warrant for 217,519 USDT stored in or accessible in Target Wallet 3. To seize the applicable USDT, Tether will "burn" (i.e., destroy) the USDT tokens currency associated with the cryptocurrency wallet and reissue the equivalent amount of USDT tokens and transfer that equivalent amount to a government-controlled cryptocurrency wallet. In accordance with this process, Tether transferred the Defendant Property to a U.S. government-controlled wallet between March and April 2025.

5. This affidavit is based on my personal knowledge, information provided by other law enforcement officers and government employees, and information gathered during this investigation including interviews of victims, the review of documents, and conversations with other law enforcement officers. This affidavit is not intended to set forth all of the information that I have learned during this investigation but includes only the information necessary to establish probable cause for the forfeiture of the Defendant Property.

BACKGROUND ON CRYPTOCURRENCY

6. Based on my training and experience, I am familiar with relevant terms and definitions discussed below.

7. 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[2] currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrencies are Bitcoin, Litecoin, Monero and Ethereum. 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, 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.[3]

8. ETH is a cryptocurrency similar to Bitcoin[4] that runs on the Ethereum blockchain as opposed to the Bitcoin blockchain. Payments or transfers of value made with ETH are recorded in the Ethereum blockchain and thus are not maintained by any single administrator or entity. As mentioned above, individuals can acquire ETH through exchanges (*i.e.*, online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat

[2] Fiat currency, such as the U.S. dollar, is backed by a government, but not by a physical commodity such as gold.
[3] 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.
[4] Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and "bitcoin" (with a lowercase letter b) to label units of the cryptocurrency. That practice is adopted here.

currencies or other cryptocurrencies), bitcoin ATMs, or directly from other people. Individuals can also acquire cryptocurrencies by "mining." An individual can "mine" bitcoins by using his or her computing power to solve a complicated algorithm and verify and record payments on the blockchain. Individuals are rewarded for this task by receiving newly created units of a cryptocurrency. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity.

9. Ethereum is a well-known blockchain that can be used to create different cryptocurrencies. There are many Ethereum-based cryptocurrencies that utilize the Ethereum blockchain, which are referred to in the cryptocurrency community as "tokens." Each Ethereum-based token has its own coding (or "smart contract") that governs how the token will operate. Tokens built using the Ethereum blockchain are fungible, meaning they can be exchanged with other Ethereum-based tokens.

10. Stablecoins are a type of virtual currency whose value is pegged to a commodity's price, such as gold, or to a fiat currency, such as the U.S. dollar, or to a different virtual currency. For example, USDT is a stablecoin pegged to the U.S. dollar. Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives.

11. 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 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. Each public address is controlled and/or accessed using 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.

12. Although cryptocurrencies such as ETH have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes, including money laundering, and is an oft used means of payment for illegal goods and services on hidden services websites operating on the Tor network.

13. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile and online wallets are electronic in nature, they are located on mobile devices (*e.g.*, smart phones

or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet.

14. Cryptocurrency exchanges are individuals or companies that exchange cryptocurrency for other currencies, including U.S. dollars. According to the Department of Treasury, Financial Crimes Enforcement Network ("FinCEN") Guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses.[5] Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). From my training and experience, I know that registered money transmitters are required by law to follow Bank Secrecy Act ("BSA") anti-money laundering ("AML") regulations, "Know Your Customer" ("KYC") protocols, and other verification procedures similar to those employed by traditional financial institutions. For example, FinCEN registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and the full bank account and routing numbers that the customer links to an exchange account.

BACKGROUND ON CRYPTOCURRENCY INVESTMENT SCHEMES

15. "Pig butchering" cryptocurrency investment schemes involve criminal actors engaging in social engineering, which allows the criminal actors to steal victims' funds through virtual currency payments and/or fraudulent investments. The phrase "pig butchering" is translated from the Chinese "shāzhūpán" and refers to a scam in which the victim is "fattened up prior to slaughter." Pig butchering scams typically involve four stages. First, a perpetrator will

[5] See "Application of FinCEN's Regulations to Person Administering, Exchanging, or Using Virtual Currencies," available at https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering.

use a fictious identity and cold-contact a victim, often via text message or messaging application, social media, a dating application, or other communication platform. Oftentimes, the perpetrator will pretend to have contacted the wrong number but will continue communicating with the victim. Second, the perpetrator will establish a relationship and build trust with the victim by continuing to message over days, weeks, or months. Third, the perpetrator will concoct a narrative to induce the victim to send a series of payments in the form of virtual currency. Common narratives include lucrative investment opportunities or emergencies necessitating funds. Many perpetrators will convince victims to use fraudulent websites or applications, controlled by scammers, to invest in virtual currency. Perpetrators coach victims through the investment process, show them fake profits, and encourage victims to invest more. In the fourth stage, perpetrators disengage victims once they have stolen their funds. In scenarios when victims stop sending more payments, the perpetrator cuts off all contact. In schemes involving fraudulent investment platforms, victims are often told they need to pay a fee or tax when they attempt to withdraw their money. Victims are then unable to get their money back from perpetrators, even if they pay the fake fees or taxes.

PROBABLE CAUSE

16. As set forth below, there is probable cause to believe that the Defendant Property represents proceeds obtained through violation of 18 U.S.C. § 1343 (wire fraud) and/or is property involved in violation of 18 U.S.C § 1956 (money laundering).

17. Pursuant to 18 U.S.C. § 981(a)(1)(C), property, real or personal, which constitutes or is derived from proceeds traceable to a violation of a specified unlawful activity, specifically violations of 18 U.S.C. § 1343 (Wire Fraud), is subject to civil forfeiture. Pursuant to 18 U.S.C. § 1961(1), as incorporated by 18 U.S.C. § 1956(c)(7)(A), violations of 18 U.S.C. § 1343 are a specified unlawful activity. It is a violation of 18 U.S.C. § 1343 for a person to devise and

intend to devise a scheme and artifice to defraud for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises, to transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing the scheme to defraud.

18. Pursuant to 18 U.S.C. § 981(a)(1)(A), property, real or personal, involved in a transaction or attempted transaction, here, violations of 18 U.S.C. § 1956(a)(1)(B)(i) and (h) (money laundering and conspiracy to commit money laundering) or property traceable to such property is subject civil forfeiture. It is a violation of 18 U.S.C. § 1956(a)(1)(B)(i) (laundering of monetary instruments) to conduct or attempt to conduct a financial transaction knowing that the transaction is designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of a specified unlawful activity. It is a violation of 18 U.S.C. § 1956(h) to conspire to engage in the offense of money laundering.

The Scheme to Defraud

19. In the fraud scheme involving the four victims discussed below, unknown subjects (the "Target Subjects") communicated with the victims first through what appeared to be misdirected text messages on their phone or through encrypted messaging applications such as WhatsApp and Telegram. After cultivating a relationship, the Target Subjects, who usually appear to be one individual, but may not be only one individual, then transferred communications with the victims to WhatsApp and Telegram. Through these communications, the Target Subjects convinced the victims to invest in an exclusive Ethereum ("ETH") investment opportunity that the Target Subjects claimed was backed by physical gold. The Target Subjects then directed victims to open accounts at various cryptocurrency exchanges such as Crypto.com, Coinbase, Kraken, and others.

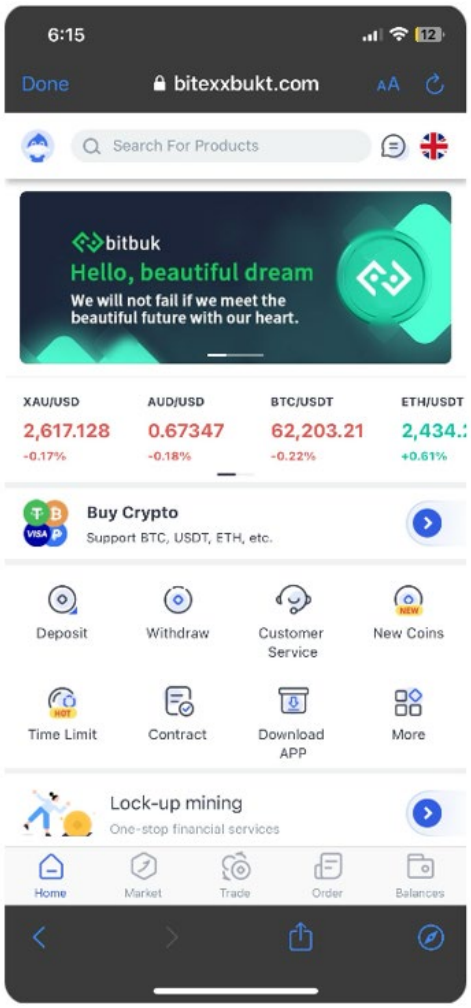
20. Once the Target Subjects had established that victims had funded their accounts at cryptocurrency exchanges, the Target Subjects then directed the victims to purchase ETH and transfer the currency to intermediary wallets controlled by the Target Subjects. The victims believed they were investing in a legitimate platform, when in fact the Target Subjects[6] were instead sending victim funds to intermediary wallets, converting victim funds from ETH into USDT, and transferring to unhosted wallets, and stealing the funds.

21. Based on my training and experience, I am aware that fraudsters and money launderers will often change the form of cryptocurrency in an effort to obscure the source of the funds and make tracing transfers of funds more difficult. Fraudsters and money launderers often used decentralized exchanges that do not do not require KYC documentation to change the form of cryptocurrency. I am also aware that fraudsters and money launderers will transfer funds to stablecoins such as USDT to avoid market volatility of other forms of cryptocurrency, such as BTC and ETH. Based on my training and experience, I am aware that fraudsters and money launderers will often use intermediary hops or transfers to intermediary wallets to try to obscure the source of the funds and make tracing the transfers of funds more difficult.

22. Based on my training and experience, I am aware that scammers in cryptocurrency investment schemes utilize websites and applications that appear to show an investment platform with victims' account balance and profit information, but in reality, the website or application and any balance and profit information are entirely fraudulent. Here, the Target Subjects used a purported investment platform, referred to as "BITBUKCS" or "BITBUK" and its associated website (www.bitexxbukt.com), which appears to have been

[6] It could be that the same individual or individuals communicating with the victims cause the transfer of funds, or it could be done by other unknown subjects working in conjunction with those who are communicating with the victims directly. For purposes of this affidavit, Target Subjects refer to all unknown subjects participating in the fraud scheme.

created by the Target Subjects for the sole purpose of deceiving victims and facilitating the fraud scheme. I have viewed www.bitexxbukt.com, and it appears to resemble a standard cryptocurrency trading platform, aside from displaying the name "bitbuk". Below is a screenshot of what Victim 1 saw on their mobile phone when accessing the website:



23. Based on my training and experience, I know that fraudsters commonly spoof the names of legitimate companies in order to gain trust from victims. I believe that the name "bitbuk" was intentionally similar in spelling to "BitBucks", which is a legitimate mobile payment application for cryptocurrency smartphone payments. Multiple variations of this website have been reported by several victims of fraud. Based on open-source records,

www.bitexxbukt.com was created on or about October 3, 2024, by a domain registrar company based in Singapore.

24. After Victim 1 reported being a victim of a cryptocurrency investment fraud, and law enforcement traced funds from that scam to Target Wallet 1 and Target Wallet 2, the FBI utilized forensic tracing techniques to backtrace transactions that were sent to Target Wallet 1 and Target Wallet 2 to identify additional potential victims whose transactions were similar to Victim 1 and whose funds ended up at either Target Wallet 1 and/or Target Wallet 2. Based on records received from other cryptocurrency exchanges, the FBI has identified and interviewed three additional victims whose experiences were consistent with Victim 1.

25. The FBI also utilized forensic tracing techniques to backtrace transactions that were sent to Target Wallet 1 and Target Wallet 2. During this process, Target Wallet 3 was identified as having similar characteristics to Target Wallet 1 and Target Wallet 2.

Victim 1

26. Victim 1 is a Massachusetts resident who walked into the Woburn Police Department on or about October 10, 2024, to report that they were a victim of a cryptocurrency scam. According to information provided by Victim 1, they were in contact with an individual or individuals going by the name of "Lin lin" on Telegram, a messaging application, who introduced Victim 1 to the alleged cryptocurrency investment opportunity. Lin lin befriended Victim 1 through instant messaging and video calls, and offered emotional support to Victim 1 to obtain their trust. Lin lin told Victim 1 that she could help them earn money in cryptocurrency investments that were backed by actual gold prices. Lin lin told Victim 1 that she was the head of cosmetology at a beauty company and that Lin lin's aunt was in finance and had introduced Lin lin to the investment world. Lin lin walked Victim 1 through the process of opening a

Crypto.com account and told Victim 1 how to access the internet platform "BITBUK". At the Target Subjects' direction, Victim 1 made approximately 22 transactions totaling approximately 34.15 ETH ($85,667.29) from their Crypto.com DeFi[7] wallet to BITBUK between August 26 and October 9, 2024.[8]

27. Using forensic tracing techniques, law enforcement was able to trace Victim 1's transactions. Each of the 22 transactions generally fell into the following pattern:

a. Victim 1, at the direction of the Target Subjects, would transfer funds into their Crypto.com DeFi wallet.

b. From Victim 1's DeFi wallet, the funds were moved by the Target Subjects through an intermediary hop (or transfer) to an unhosted wallet. From the intermediary hop, the Target Subjects moved Victim 1's funds to Target Wallet 1.

c. From Target Wallet 1, Victim 1's funds were swapped from ETH into USDT using a decentralized exchange[9], and sent to Target Wallet 2 as USDT.

d. During this process, Victim 1 believed that they were investing in a gold-backed cryptocurrency investment in ETH, while the Target Subjects were moving

[7] Crypto.com offers a DeFi wallet that is now known as Crypto.com "Onchain". Onchain is a non-custodial wallet that gives users access to DeFi services such as trading, swapping, storage, and staking. Users can swap over 1,000 tokens across multiple blockchains. Onchain can be connected from a mobile application on a phone and linked to a desktop browser. Users can send and receive crypto, view balances, and confirm transactions.

[8] The price of ETH was approximately $2,682 on August 26, 2024 and $2,368 on October 9, 2024.

[9] Tokenlon and FixedFloat are two examples of decentralized exchanges or exchange platforms that allow users to exchange cryptocurrencies and tokens. Both Tokenlon and FixedFloat do not require KYC documentation and were used by the Target Subjects to facilitate the cryptocurrency investment scheme.

Victim 1's funds from Victim 1's control without their knowledge or permission, converting Victim 1's funds into USDT, and stealing the funds.

28. The Target Subjects utilized a website www.bitexxbukt.com which was provided to Victim 1, and where Victim 1 could log in to view their investment contributions and alleged profits. Any balance or profits displayed to Victim 1 on this website were false, and no funds were ever invested per Victim 1's wishes and agreement with the Target Subjects. Forensic tracing of Victim 1's 34.15 ETH ($85,667.29) traced Victim 1's funds to USDT in Target Wallet 1 and Target Wallet 2.

Victim 2

29. Victim 2, a Massachusetts resident, met an individual or individuals calling themselves "Anita", via a misdirected text message around August 2024. Anita moved the conversation from text messaging to WhatsApp, and then to Telegram. Anita cultivated a relationship with Victim 2, built trust with Victim 2, and eventually convinced Victim 2 to invest in the gold market via cryptocurrency through a trading platform known as "Bitbukcs" [10].

30. The Target Subjects instructed Victim 2 to download the Bitbukcs mobile application ("app") and also the Kraken application (Kraken is an actual cryptocurrency exchange). Victim 2 had never purchased or traded in cryptocurrency and did not have a Kraken account prior to speaking with the Target Subjects.

31. Kraken records showed that Victim 2 created an account on or about May 17, 2024. Between May 17, 2024, and June 20, 2024, Victim 2 purchased approximately 10.09 ETH

[10] Based on my training and experience, I know that criminals often change the names of fraudulent websites to avoid detection by law enforcement. Therefore, it is likely that "Bitbuk", "Bitbuks", "Bitbukcs", and other misspelled variations are referring to the same platform controlled by the Target Subjects.

($34,838.69). Forensic tracing revealed that all of Victim 2's funds were sent to Target Wallet 1, and approximately 8.49 of Victim 2's ETH was in Target Wallet 1 when it was seized.

32. When Victim 2 had issues while using Kraken (*e.g.*, setting up an account, purchasing cryptocurrency), Victim 2 would contact Kraken's customer service. The Target Subjects, however, coached Victim 2 on what to say to Kraken's customer service to prevent their account form being flagged and/or disabled. When Victim 2 had some issues sending cryptocurrency, the Target Subjects instructed Victim 2 to send wire transfers to both domestic and international accounts. Some of the international wires were addressed to Southeast Asian countries.

33. After completing some wire transfers, Victim 2 was told by Target Subjects that their credit was harmed as a result of an insider trading investigation and that Victim 2 would need to pay approximately $42,000 to repair their credit. At one point, Victim 2 was also told that they needed to pay a fine and/or fee to complete a withdrawal of Victim 2's funds. Victim 2 was told if they paid an additional $60,000 then they would receive their investment immediately. Victim 2 was then instructed to send more than $200,000 in additional funds, which they did not do.

34. Between cryptocurrency and wire transfers, Victim 2 sent approximately $100,000 to the scammers. Approximately $29,992.41 of Victim 2's funds were in Target Wallet 1 at the time of seizure.

Victim 3

35. Victim 3, a Utah resident, met an individual or individuals calling themselves "Karina" via a misdirected text message on or about August 21, 2024. Shortly thereafter, "Karina" moved the conversation to Telegram. Karina then began discussing cryptocurrency

gold investments with Victim 3 and convinced Victim 3 to invest. Victim 3 believed they were investing in the gold market using the trading platform known as "Bitbukcs". Victim 3 was provided with a link to Bitbukcs' website located at www.bitexxbukt.com to create an account and monitor the investment. Victim 3 did not believe they were investing in any particular cryptocurrency, rather they believed they were making trades based solely on the gold market.

36. Victim 3 was directed to send approximately $94,000 via wire transfers to financial accounts in Vietnam and Japan and send approximately $6,000 in cryptocurrency from Victim 3's Crypto.com account. Victim 3's wire transfers and crypto transactions occurred on or about the following dates:

a. According to records received from Crypto.com and Victim 3's statements, between August 24 and September 7, 2024, Victim 3 converted existing cryptocurrency into ETH and was directed to send approximately 2.53 ETH ($6,190.23) across four transactions to a cryptocurrency address which Victim 3 believed was the "Bitbukcs" platform. Forensic tracing revealed that Victim 3's funds were converted to USDT and ultimately ended up at Target Wallet 1.

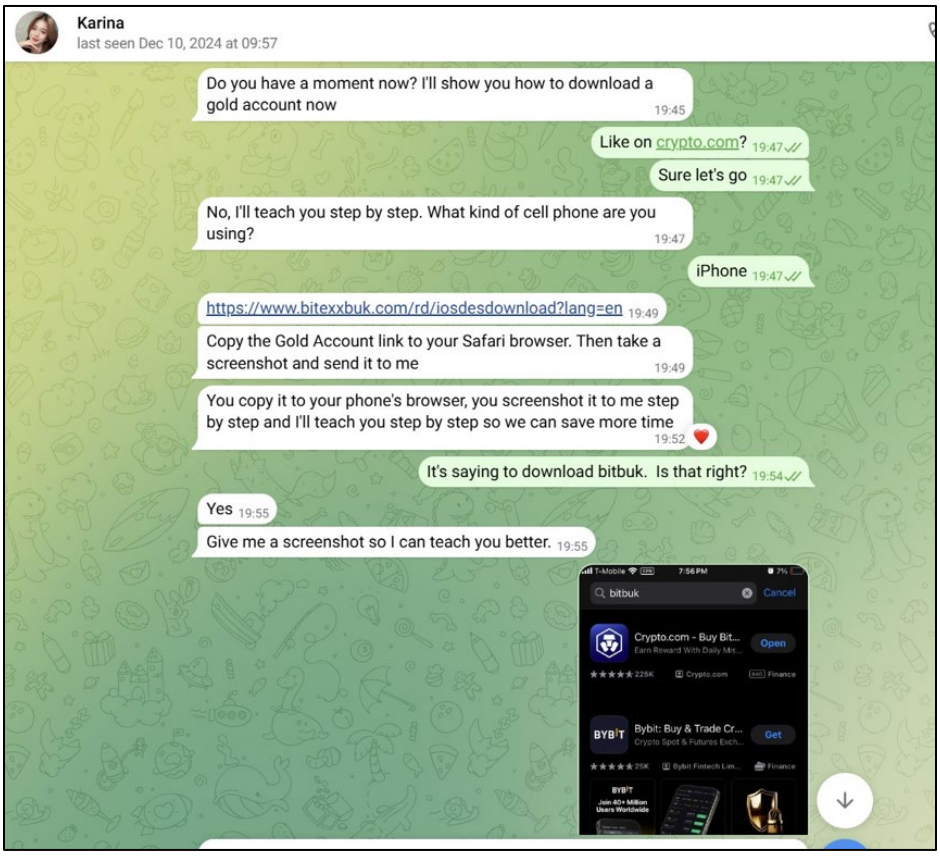
b. On September 5, 2024, Victim 3 sent a $14,000 wire transfer to a bank account in Ho Chi Minh City, Vietnam. Victim 3 received confirmation through WhatsApp messages with Bitbukcs customer service that this transaction was received.

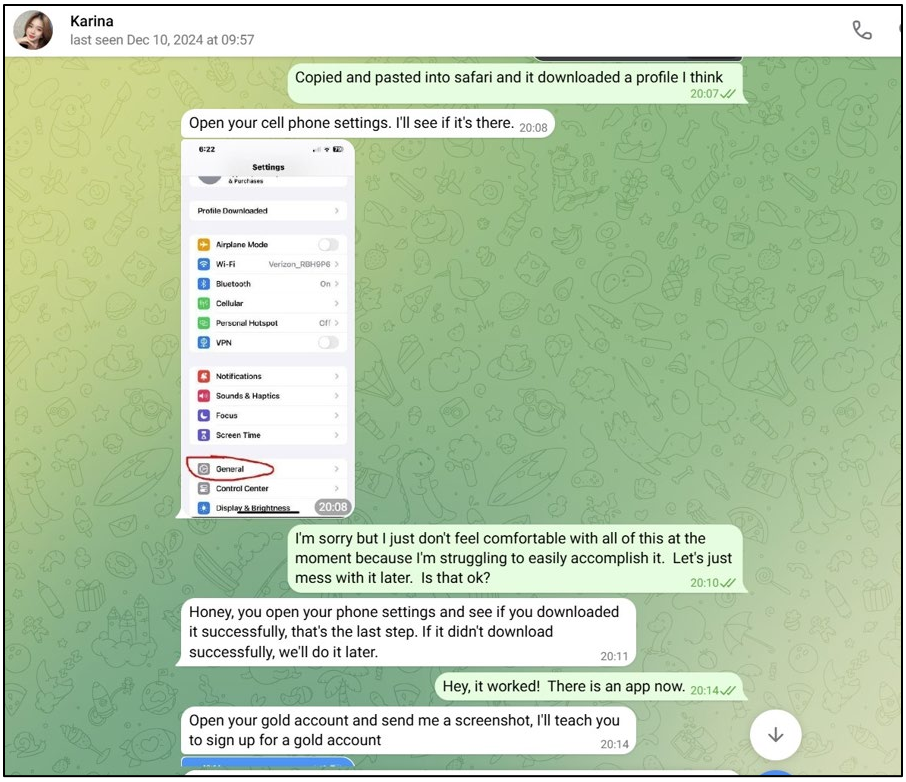
c. On October 4, 2024, Victim 3 sent an $80,000 wire transfer to a bank account in Tokyo, Japan. Victim 3 received confirmation that this transaction was received through WhatsApp messages with Bitbukcs customer service.

Victim 3 believed the above wire transfers and cryptocurrency transactions were being deposited into their Bitbukcs account, as the deposits subsequently appeared on the Bitbukcs platform

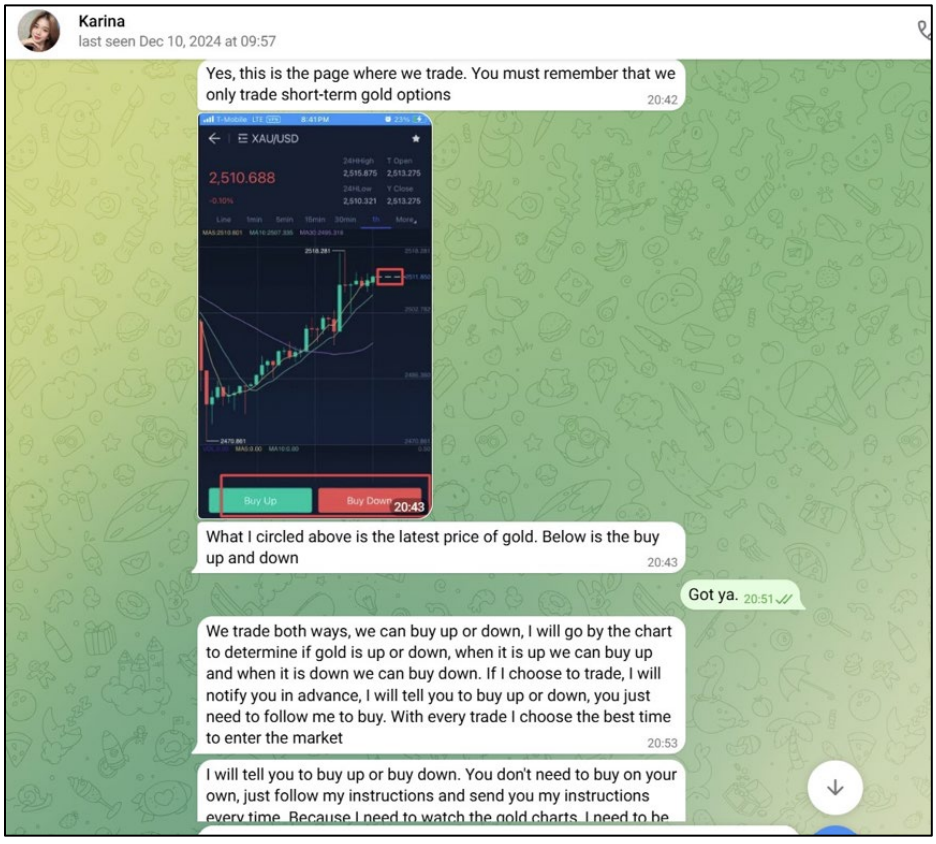
linked to Victim 3's account. Victim 3's last contact with any alleged Bitbukcs representatives was on or about October 20, 2024.

37. Below is an example of Victim 3 being recruited by an individual promoting Bitbukcs through messaging on Telegram, including step by step instructions on how to access and download the application, and how to begin trading:

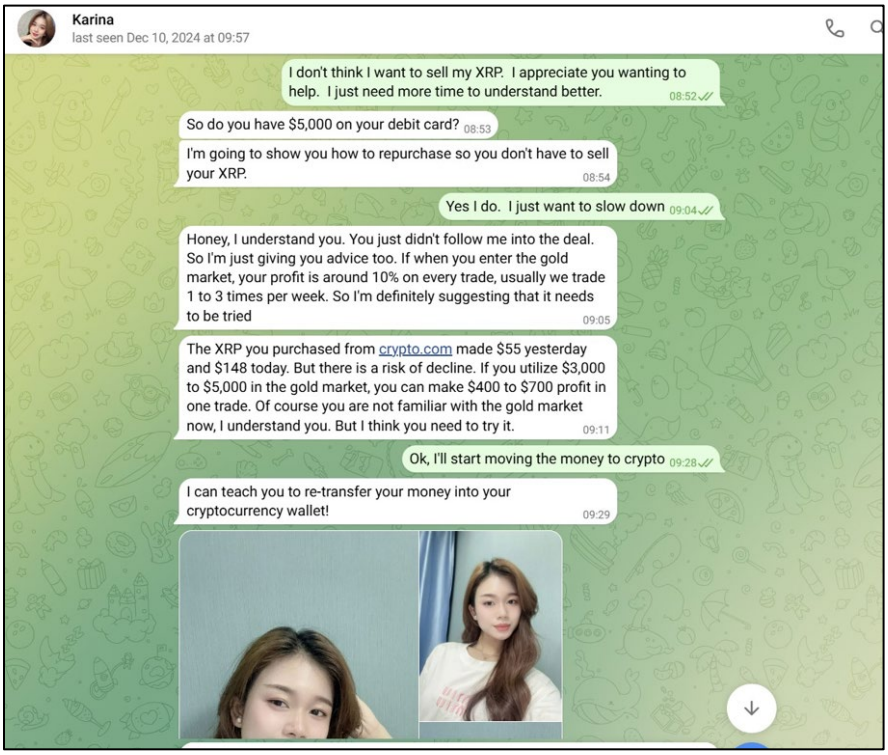




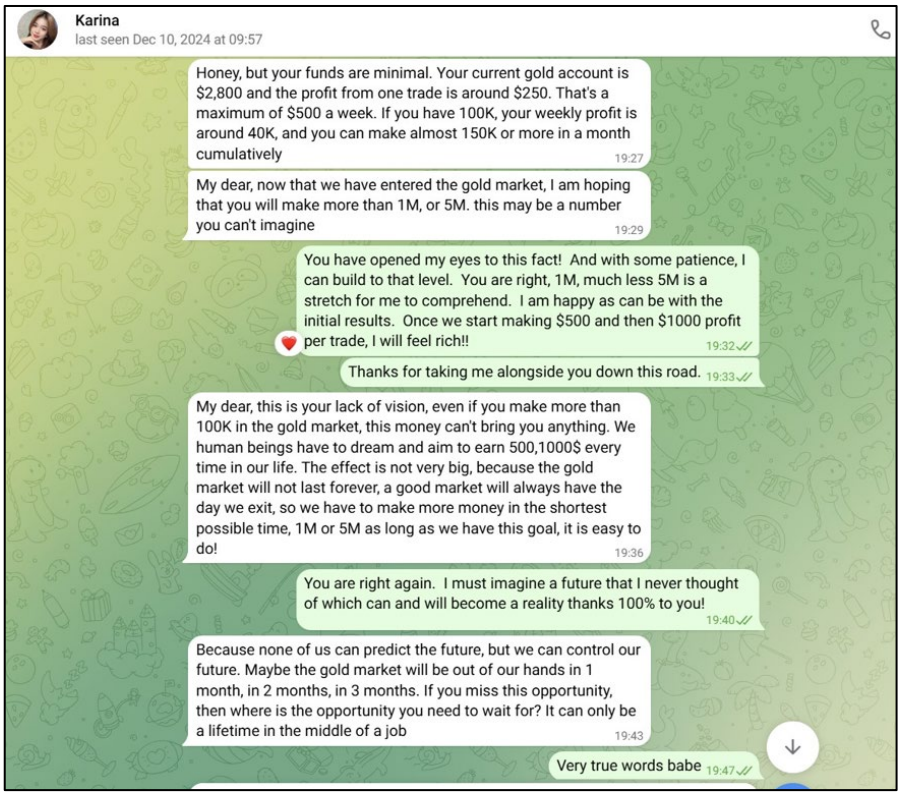
38. Below is an example of the fraudulent trading platform:



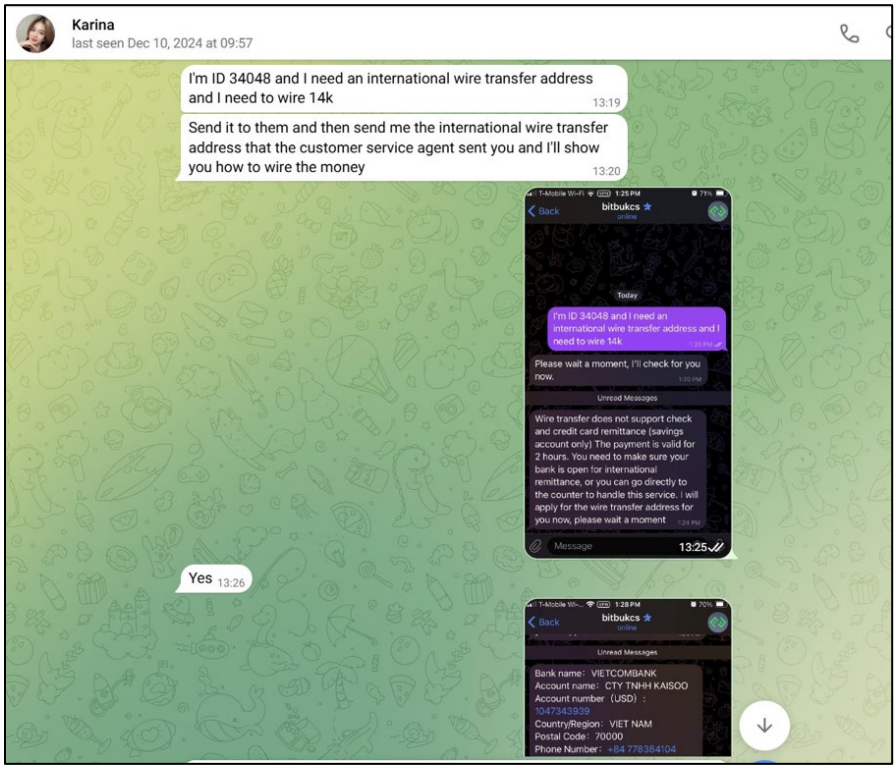
39. At times, Victim 3 expressed concern about investing:



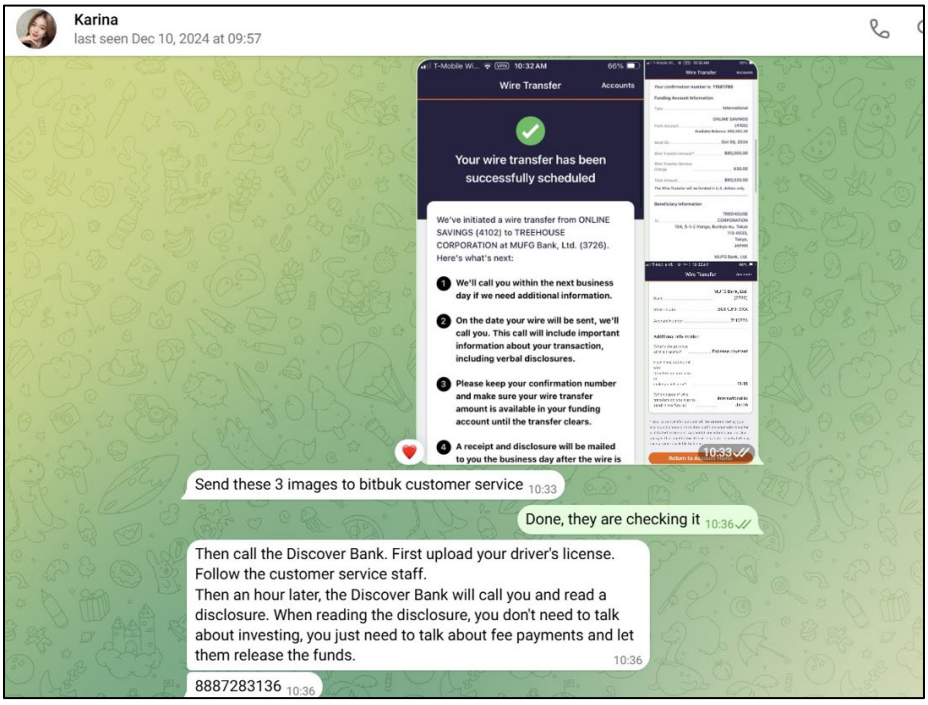
40. Victim 3 was convinced to invest more with the promise of significant profits:



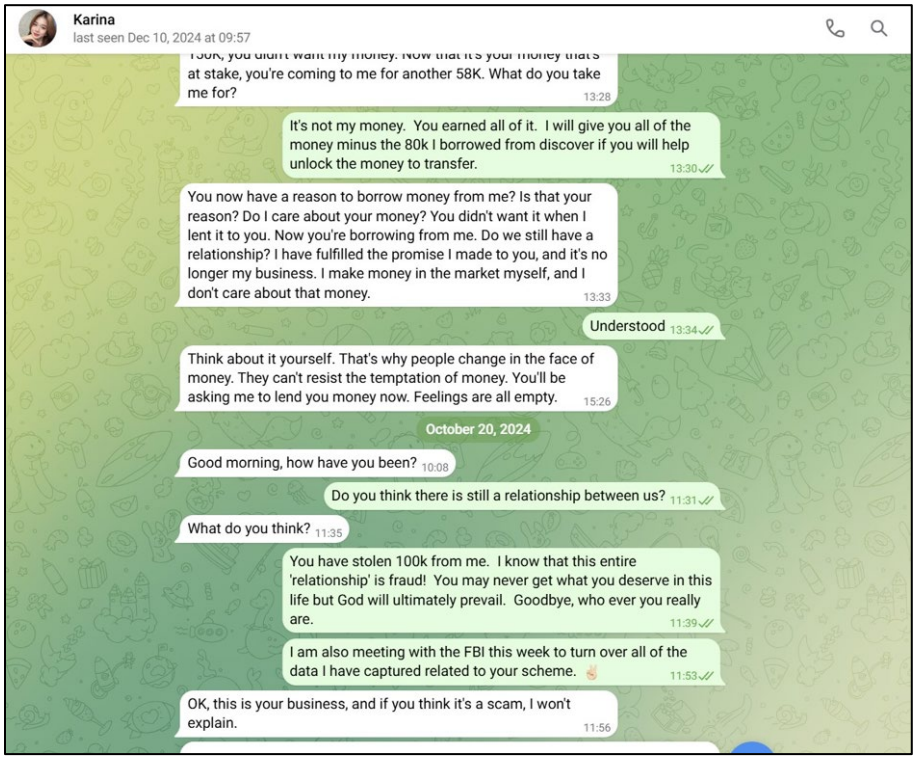
41. Victim 3 was instructed to converse with the "Customer Service" to fund Victim 3's Bitbukcs account:



***



42. Ultimately, Victim 3 realized that the entire platform was fraudulent, and they confronted the Bitbukcs representative:



Victim 4

43. Victim 4, a South Carolina resident, met a person named "Lin Lin Tan" around October 2024 through a misdirected text message. Soon after, Tan transitioned the conversation to Telegram and told Victim 4 that she could help them make money trading gold futures contracts through a platform called "Bitbuk". Victim 4 would send text messages through Telegram either every other night or twice per week from October through November 2024. To invest money, Victim 4 would wire funds into their Crypto.com or Coinbase account, then, as directed by Tan, transfer the funds to a wallet address which was provided by Tan.

44. When Victim 4 attempted to withdraw a portion of their funds from the Bitbuk platform around the holidays, the Target Subjects told Victim 4 they needed to pay an additional $70,000 verification fee to act as a security deposit. Victim 4 was also told that their "credit

score[11]" went down, and in order to restore their credit, Victim 4 needed to pay an additional $20,000. In total, Victim 4 estimated that they had transferred $200,000 of their own money into Bitbuk, which represents almost everything that Victim 4 had saved.

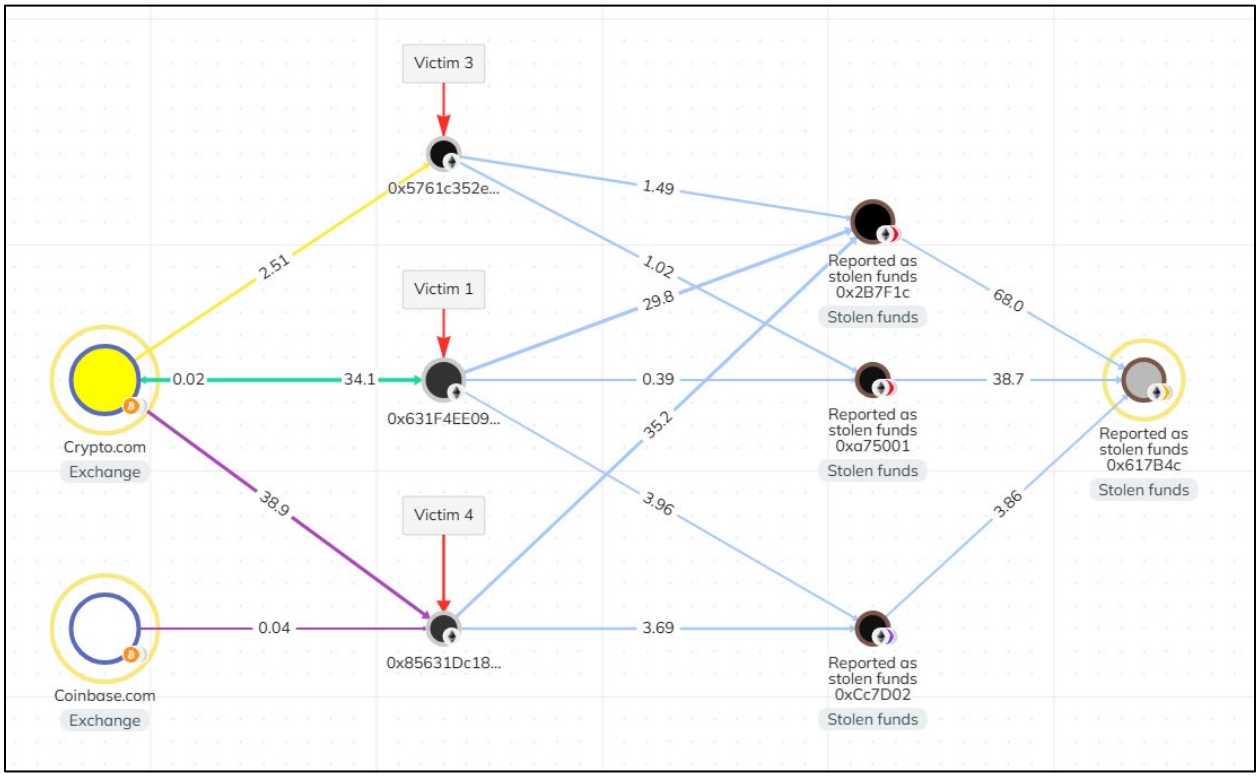
45. Records received from Crypto.com showed that between October 25 and December 17, 2024, Victim 4 purchased approximately 54.71 ETH ($172,931.82) and sent the funds to unhosted wallets. Approximately $67,247.47 of Victim 4's funds were traced to Target Wallet 1. Additional forensic tracing and records received from Crypto.com and Coinbase showed that 11.19 ETH ($34,947.58) of Victim 4's funds were traced to Target Wallet 3.

GRAPHICAL REPRESENTATION OF THE FLOW OF VICTIM FUNDS

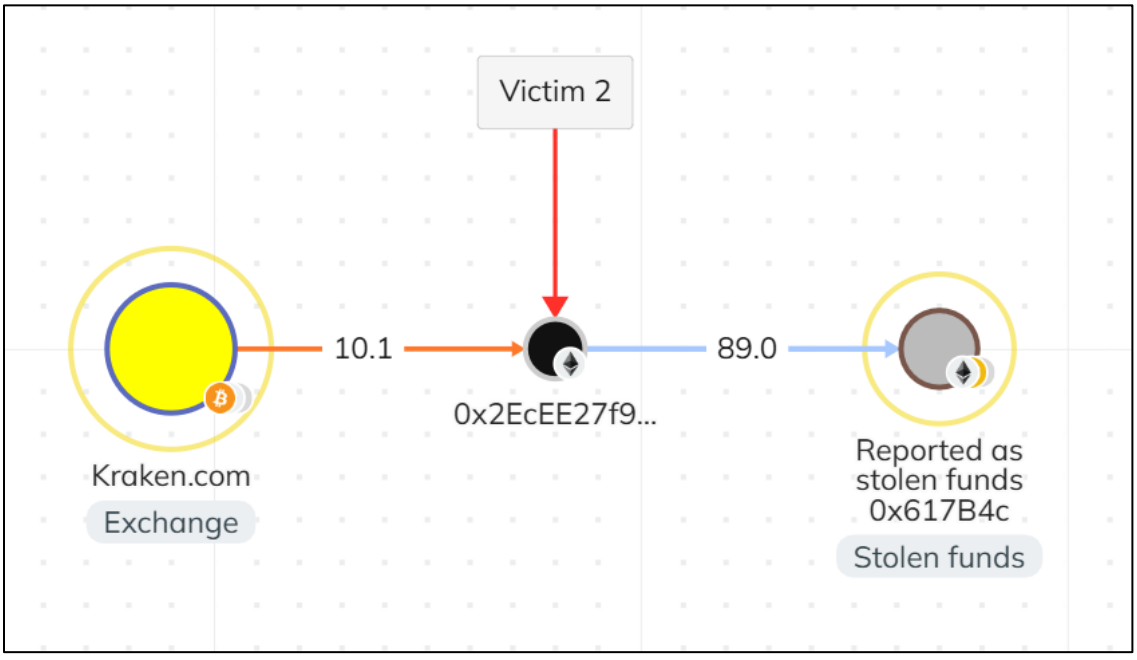
46. Below is a chart showing the flow of funds from Victims 1, 3, and 4 from their cryptocurrency accounts at Crypto.com and Coinbase to intermediary unhosted wallets and

[11] Through my interviews with the victims, I have learned that "credit score" is a feature unique to Bitbuk and does not refer to the individuals' actual credit score through the traditional credit reporting agencies.

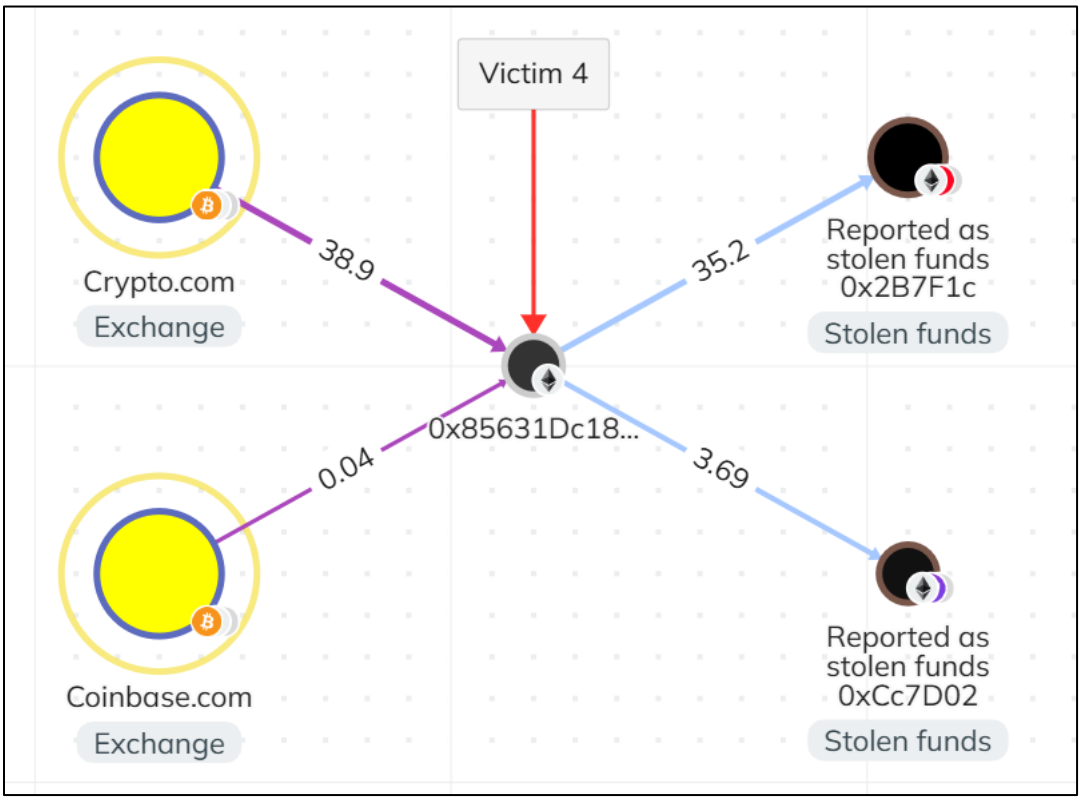
subsequently to Target Wallet 1.



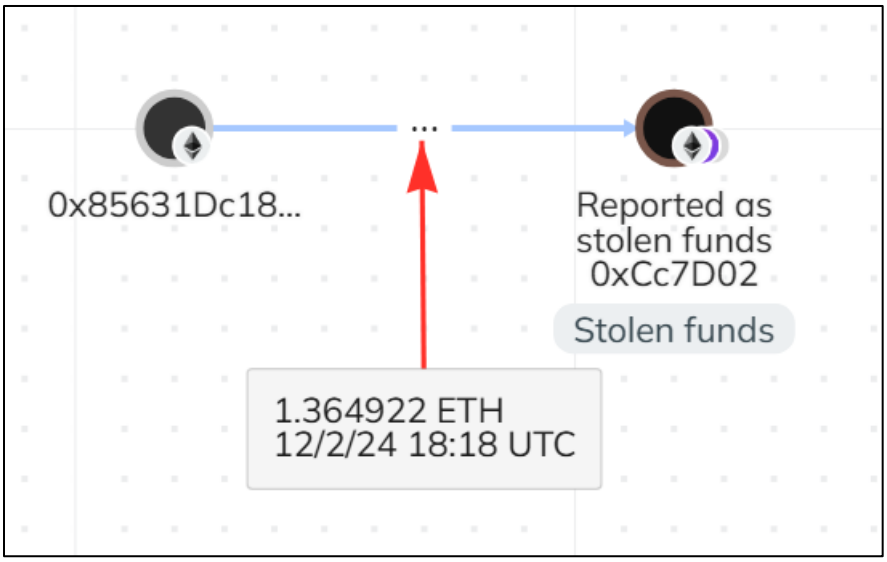
47. Below is a chart showing the flow of funds from Victim 2 whose funds were sent directly from Victim 2's cryptocurrency account at Crypto.com to Target Wallet 1.



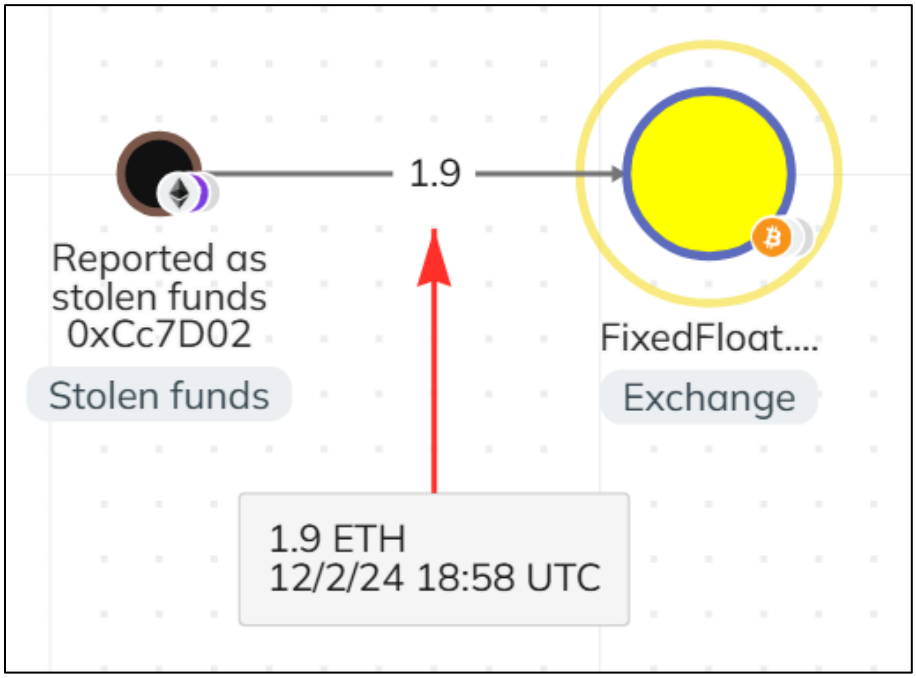
48. Below is a chart showing the flow of funds from Victim 4 whose funds were sent to intermediary unhosted wallets from their accounts at Crypto.com and Coinbase:



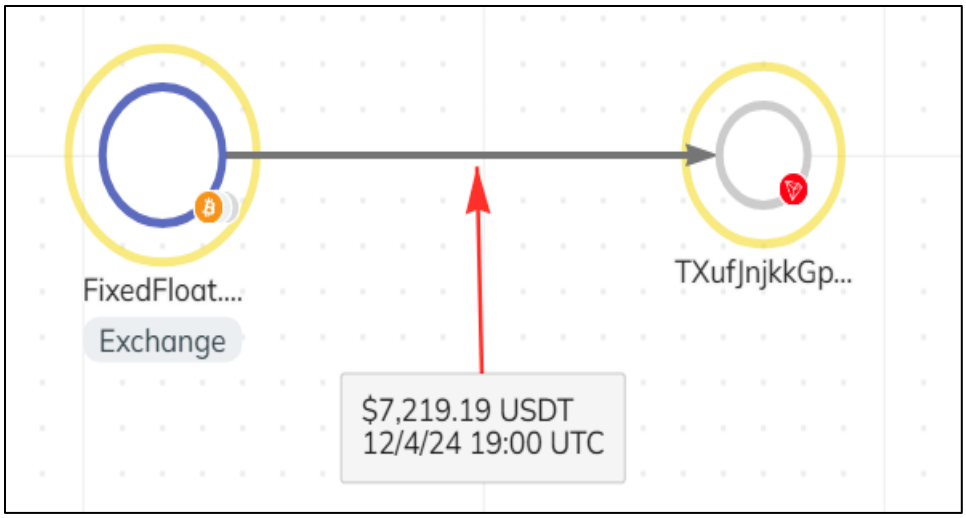
49. On December 2, 2024, Victim 4 sent approximately 1.36 ETH:



50. 40 minutes later, Victim 4's ETH was sent to FixedFloat:



51. On December 4, 2024, Victim 4's ETH was converted into USDT and sent to Target Wallet 3:



SUMMARY OF TARGET WALLETS AND COMMINGLING OF FUNDS

52. In total, Target Wallet 1 was active from August 30, 2023, through November 28, 2024, and received a total of approximately 4,984,131 USDT and sent a total of approximately 3,700,367 USDT.

53. In total, Target Wallet 2 was active from May 15, 2024, through October 28, 2024, and received a total of approximately 4,453,126 USDT and sent a total of approximately 2,509,248 USDT. Target Wallet 2 received funds from Target Wallet 1 and from other unhosted wallets that appear to have received victim funds in a similar manner to Target Wallets 1 and 2 but are not detailed in this affidavit.

54. In total, Target Wallet 3 was active from August 17, 2023, until December 16, 2024, and received a total of approximately 17,714,348 USDT, and sent a total of approximately 17,496,829 USDT.

55. Through backtracing, other potential victims in addition to victims 1 through 4 were identified as having sent funds to Target Wallet 1. In the case of Victims 1, 3 and 4, victim ETH was transferred through multiple hops among unhosted wallets before arriving in Target Wallet 1. Once victim ETH was received, the Target Subjects utilized exchanging services such as Tokenlon to convert ETH into USDT. Once the USDT was received back in Target Wallet 1, the Target Subjects sent the USDT to Target Wallet 2.

56. Generally, Target Wallet 3 received ETH from other victims in a similar manner to Victim 4 as detailed above. Victims' ETH was transferred through multiple hops among unhosted wallets before arriving in Target Wallet 3. Once victims' ETH was received, the Target Subjects utilized exchanging services such as FixedFloat to convert ETH into USDT. The converted USDT was then received back into Target Wallet 3 and sent to various other unhosted

wallets controlled by the Target Subjects.

57. Based on my training and experience, a review of the transactions containing victim funds demonstrated that the Target Subjects displayed tactics typically used in money laundering transactions and did so for the purpose of attempting to conceal the origin of the fraud proceeds. Specifically, the Target Subjects transferred victim funds through multiple hops of unhosted wallets and converted victim funds from the original cryptocurrency (ETH), into a different cryptocurrency (USDT). Additionally, victim funds from Victims 1 through 4 received into Target Wallets 1, 2, and 3 were commingled with other backtraced victim funds as well as funds of unknown origin.

58. Accordingly, there is probable cause to believe that the Defendant Property is property involved in a violation of 18 U.S.C. § 1956 (laundering of monetary instruments) and is subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 982(a)(1).

CONCLUSION

59. Based on my knowledge, training, and experience, and the foregoing information set forth in this affidavit, I respectfully submit that there is probable cause that the Defendant Property is subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(A) and (a)(1)(C) because it represents proceeds traceable to a violation of 18 U.S.C. § 1343 (wire fraud) and is property involved in violations of 18 U.S.C. § 1956 (money laundering), or property traceable to such property.

Pursuant to 28 U.S.C. § 1746, I declare under penalties of perjury that the foregoing is true and correct to the best of my knowledge, information, and belief. Executed this 4th day of March, 2026.

Respectfully submitted,

Michael Jankowiak
Special Agent
Federal Bureau of Investigation