**UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF COLUMBIA**

| | |
|---|---|
| **UNITED STATES OF AMERICA,**<br><br>**Plaintiff,**<br><br>**v.**<br><br>**APPROXIMATELY 225,364,961 USDT**<br><br>**Defendant *in rem*.** | **Civil Action No. 25-cv-1907** |

**VERIFIED COMPLAINT FOR FORFEITURE *IN REM***

Plaintiff, the United States of America, through the U.S. Attorney for the District of Columbia, brings this verified complaint for forfeiture in a civil action *in rem* against 225,364,961 USDT, hereinafter Defendant Property, and alleges as follows:

**STATEMENT OF THE CASE**

1. Criminals abroad, along with their associates and conspirators, stole funds from over 430 suspected victims. After stealing those funds, the criminal actors laundered them through a convoluted web of cryptocurrency accounts and addresses to evade detection and to hide the fact that the funds came from victims. The United States Secret Service ("USSS") and the Federal Bureau of Investigation ("FBI") used blockchain analysis and other investigative techniques to identify, freeze, and seize the Defendant Property, which constitutes proceeds traceable to those thefts and property involved in, and traceable to, this money laundering scheme.

2. The United States of America seeks to lawfully forfeit the Defendant Property to punish and deter criminal activity by depriving criminals of property used in or acquired through

illegal activities; to promote and enhance cooperation among federal and foreign law enforcement agencies; and most importantly, to recover assets that may be used to compensate victims.[1]

**JURISDICTION AND VENUE**

3. 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.

4. This Court has *in rem* jurisdiction over the Defendant Property under 28 U.S.C. § 1355(b).

5. Venue is proper in this judicial district under 18 U.S.C. § 3238 and 28 U.S.C. §§ 1355(b) and 1395(a), (b), and (c).

**NATURE OF THE ACTION AND STATURY BASIS FOR FORFEITURE**

6. The United States files this *in rem* forfeiture action to seek forfeiture of Defendant Property as constituting proceeds of wire fraud and wire fraud conspiracy offenses, committed in violation of 18 U.S.C. §§ 1343, 1349, 2, and 3, and as involved in money laundering and money laundering offenses, committed in violation of 18 U.S.C. 1956(a)(1)(B)(i), 1956(h), and 2, and 3.

7. Procedures for this action are mandated by Rule G of the supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions and, to the extent applicable, 18 U.S.C. §§ 981 and 983 and the Federal Rules of Civil Procedure.

8. 18 U.S.C. § 981(a)(1)(A) mandates forfeiture of any property, real or personal, involved in a transaction or attempted transaction in violation of section 18 U.S.C. §§ 1956, 1957,

[1] U.S. Department of Justice, *Asset Forfeiture Program*, https://www.justice.gov/afp. (Last accessed Jun. 17, 2025).

or 1960, or any property traceable to such property.

9. 18 U.S.C. § 981(a)(1)(C) mandates forfeiture of property constituting or derived from proceeds traceable to wire fraud, conspiracy to commit wire fraud, or any offense constituting "specified unlawful activity" as defined by 18 U.S.C. § 1956(c)(7), or a conspiracy to commit such offense. A violation of 18 U.S.C. § 1343, or a conspiracy to commit that offense, constitutes specified unlawful activity under 18 U.S.C. § 1956(c)(7)(A) as an offense listed in 18 U.S.C. § 1961(1)(B).

10. Title 18 U.S.C. § 1343 provides that whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, commits the violation of wire fraud.

11. Title 18 U.S.C. § 1349 provides that whoever attempts or conspires to commit a violation of 18 U.S.C. § 1343 shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy.

12. Title 18 U.S.C. § 1956(a)(1)(B)(i) provides in relevant part that whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts 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, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity" is guilty of concealment money laundering.

13. Title 18 U.S.C. § 1956(h) provides that any person who conspires to commit any offense of 1956 or 1957 is subject to the same penalties as those prescribed for the offense the commission of which was the object of the conspiracy.

14. Title 18 U.S.C. § 1956(f) provides extraterritorial jurisdiction over prohibited conduct in Section 1956 if the conduct is by a United States citizen, or by a non-United States citizen and the conduct occurs in part in the United States and the transaction or series of related transactions involves funds or monetary instruments of a value exceeding $10,000.

**PROPERTY INFORMATION**

15. The Defendant Property consists of the following:

| **Virtual Currency Address:** | **Virtual Currency Amount** | **Defined Term** |
|---|---|---|
| 0xc7c8f8284c5360d0086a2f0a05bdd07afde23246 | 29,413,680.82 USDT | "USDT Token Group A" |
| 0x564e11ace70bfe6c943a973f1289faa6e8a0fe16 | 30,000,000.35 USDT | "USDT Token Group B" |
| 0xcab9a8391f765f6beda0b5bad434b10985bdaad0 | 8,737,741.569083 USDT | "USDT Token Group C" |
| 0x0b5453635e5325f5385ca1643c9e9eb173f9d5a8 | 2,903,914.212488 USDT | "USDT Token Group D" |
| 0xc76afbf0f69ae9be5d855239c50673252cf3f26b | 2,137,276.136 USDT | "USDT Token Group E" |
| 0x99ebaf3661065dc1e44feff4b80365678bdff6ce | 64,707,708.53 USDT | "USDT Token Group F" |
| 0x82e1d4ddd636857ebcf6a0e74b9b0929c158d7fb | 87,464,642.259005 USDT | "USDT Token Group G" |

The above virtual currency addresses are hereinafter collectively referred to as "**SUBJECT VIRTUAL CURRENCY ADDRESSES.**" Altogether, the amount of virtual currency associated with the **SUBJECT VIRTUAL CURRENCY ADDRESSES** is referred to as "Defendant

Property."

16. The Defendant Property is currently in the custody of the United States Marshals Service in the District of Columbia.

## BACKGROUND ON VIRTUAL CURRENCY

17. **Virtual Currency**: Virtual currencies are digital representations of value that, like traditional coin and paper currency, function as a medium of exchange (i.e., they can be digitally traded or transferred and can be used for payment or investment purposes). Virtual currencies are a type of digital asset separate and distinct from digital representations of traditional currencies, securities, and other traditional financial assets. The exchange value of a particular virtual currency generally is based on agreement or trust among its community of users. Some virtual currencies have equivalent values in real currency or can act as a substitute for real currency, while others are specific to particular virtual domains (e.g., online gaming communities) and generally cannot be exchanged for real currency. Cryptocurrencies, like Bitcoin (or BTC) and Ether (or ETH), are types of virtual currencies, which rely on cryptography for security. Cryptocurrencies typically lack a central administrator to issue the currency and maintain payment ledgers. Instead, cryptocurrencies use algorithms, a distributed ledger known as a blockchain, and a network of peer-to-peer users to maintain an accurate system of payments and receipts.

18. **Blockchain**: A blockchain is a digital ledger run by a decentralized network of computers referred to as "nodes." Each node runs software that maintains an immutable and historical record of every transaction utilizing that blockchain's technology. Many digital assets, including virtual currencies, publicly record all of their transactions on a blockchain, including all of the known balances for each virtual currency address on the blockchain. Blockchains consist of blocks of cryptographically signed transactions, and blocks are added to the previous block after validation and after undergoing a consensus decision to expose and resist tampering or manipulation of the data. There are many different blockchains used by many different virtual currencies. For example, Bitcoin in its native state exists of the Bitcoin blockchain, while Ether exists in its native state on the Ethereum network.

19. **Blockchain Analysis**: Law enforcement can trace transactions on blockchains to determine which virtual currency addresses are sending and receiving particular virtual currency. This analysis can be invaluable to criminal investigations for many reasons, including that it may enable law enforcement to uncover transactions involving illicit funds and to identify the person(s) behind those transactions. To conduct blockchain analysis, law enforcement officers use reputable, free open source blockchain explorers, as well as commercial tools and services. These commercial tools are offered by different blockchain-analysis companies. Through numerous unrelated investigations, law enforcement has found the information associated with these tools to be reliable.

20. **Virtual Currency Address**: A virtual currency address is an alphanumeric string that designates the virtual location on a blockchain where virtual currency can be sent and received. A virtual currency address is associated with a virtual currency wallet.

21. **Intermediary Address:** An "intermediary address" in virtual currency tracing refers to a wallet address used in a virtual currency transaction that acts as a temporary stopping point between the original sender and the final recipient, often employed to obscure the true source or destination of funds by adding an extra layer of complexity to the transaction trail. Essentially, criminal actors use intermediary addresses as "middleman" addresses to obfuscate the flow of funds. The funds are transferred through the middleman/intermediary address for no legitimate purpose. This is especially obvious because each transfer requires fees, meaning it costs the criminal actors money in order to do these transactions.

22. **Virtual Currency Exchange**: A virtual currency exchange ("VCE"), also called a cryptocurrency exchange, is a platform used to buy and sell virtual currencies. VCEs allow users to exchange their virtual currency for other virtual currencies or fiat currency, and vice versa. Many VCEs also store their customers' virtual currency addresses in hosted wallets. VCEs can be centralized (i.e., an entity or organization that facilitates virtual currency trading between parties on a large scale and often resembles traditional asset exchanges like the exchange of stocks) or decentralized (i.e., a peer-to-peer marketplace where transactions occur directly between parties).

23. **Pass-Through Account:** A "pass-through" account is an account primarily used to transfer funds through a VCE's own addresses, often removing the link between the source of funds and the destination. Pass-through accounts often receive, then promptly transfer the funds without exchange activity, which is an unnecessary step that incurs transaction fees without a legitimate purpose. This effectively turns the VCE into a money laundering mixer.

24. **Virtual Currency Wallet**: A virtual currency wallet (e.g., a hardware wallet, software wallet, or paper wallet) stores a user's public and private keys, allowing a user to send and receive virtual currency stored on the blockchain. Multiple virtual currency addresses can be controlled by one wallet.

25. **Unhosted Wallet**: An unhosted wallet, also known as a self-hosted, non-custodial wallet, is a virtual currency wallet through which the user has complete control over storing and securing their private keys and virtual currency. Unhosted wallets do not require a third party's involvement (e.g., a virtual currency exchange) to facilitate a transaction involving the wallet.

26. **Decentralized Exchange**: A decentralized exchange (or "DEX") is a peer-to-peer marketplace where users can trade virtual currencies directly with other traders without centralized intermediaries. Users generally retain control over their virtual currency rather than entrusting a central authority to host funds in a centralized or "hosted" wallet. DEXs are operated by self-executing agreements written in code, known as "smart contracts," which automate the trading process. DEXs will algorithmically track the prices of various virtual currencies and often leverage locked reserves of virtual currencies (or other digital assets). These locked reserves are known as "liquidity pools," and they are often used to facilitate trades. DEXs are built on blockchains that support smart contracts, including Ethereum, and often levy fees for their services.

27. **Transaction Fee**: A transaction fee is a fee paid by the party sending virtual currency on a blockchain to reward miners and/or validators for verifying and validating transactions. Transaction fees vary by blockchain and can fluctuate based on factors such as blockchain network traffic and transaction sizes. Senders of virtual currency can increase the transaction fees that they pay to have their transactions confirmed faster by miners and/or validators. Transaction fees are generally paid in a blockchain's native token (e.g., Bitcoin on the Bitcoin blockchain). On the Ethereum network, these transaction fees are called "gas fees." Gas fees are transaction costs paid in Ether, or its fraction, gwei. These fees serve as a form of remuneration for validators who maintain and secure the network. Gas fees fluctuate based on supply, demand, and network capacity, and may increase during periods of network congestion.

28. **Stablecoins**: 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, Tether (also known as 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.

29. **Smart Contracts**: Smart contracts allow developers to create markets, store registries of debts, and move funds in accordance with the instructions provided in the contract's code, without any type of middleman or counterparty controlling a desired or politically motivated outcome, all while using the Ethereum blockchain protocol to maintain transparency. Smart contract technology is one of Ethereum's distinguishing characteristics and an important tool for companies or individuals executing trades on the Ethereum blockchain. When engaged, smart contracts automatically execute according to the terms of the contract written into lines of code. A transaction contemplated by a smart contract occurs on the Ethereum blockchain and is both

trackable and irreversible.

30. **USDT and Tether Limited:** Tether Limited ("Tether") is a company that manages the smart contracts and the treasury (i.e., the funds held in reserve) for USDT tokens.

**Background On Cryptocurrency Confidence Scams**

31. Cryptocurrency confidence scams, commonly known as "Pig Butchering," are a type of internet-based cryptocurrency investment scam. The phrase is translated from Chinese shāzhūpán and refers to a scam in which the victim is "fattened up prior to slaughter." These scams are also referred to as cryptocurrency investment fraud.[2] These types of scams typically involved four stages. *First*, a perpetrator cold contacts a victim via text, social media, or some other communication platform. Oftentimes, the perpetrator will pretend to have contacted the wrong number but continue communicating with their newfound "friend." *Second*, the perpetrator will establish a relationship with the victim by continuing to message them over days, weeks, or months. *Third*, the scammer will concoct a narrative to induce the victim to send them a series of purported investments, often in the form of cryptocurrency. These payments are often made through fraudulent investment platforms introduced by the scammer, which the victim believes to be legitimate. *Fourth*, after the victim stops sending additional payments, or begins to question the scammer about legitimacy of their "investments," the perpetrator cuts off all contact.

32. Confidence schemes are schemes where perpetrators gain trust or confidence from victims to deceive them into parting with their money. One of the most well-known forms of confidence schemes is the "romance scam," which typically features a perpetrator befriending a

[2] Federal Bureau of Investigation, *Cryptocurrency Investment Fraud,* https://www.fbi.gov/how-we-can-help-you/victim-services/national-crimes-and-victim-resources/cryptocurrency-investment-fraud?__cf_chl_rt_tk=KP0jo5lKxpcHNmC2W9IgFvxzVp58YptXkC36h1AH84I-1749423762-1.0.1.1-PrqYwbOk3o56Boyjv4_oSFvOb0GH2RnyJMQVGilzVSs (Last accessed Jun. 17, 2025).

victim through the guise of a romantic relationship, often solely existing online, in an effort to siphon funds from the victim's bank accounts or assets.

33. Cryptocurrency confidence scams feature elements of well-established investment schemes blended with fraudulent websites, mobile apps, or dApps[3] and the opaqueness of cryptocurrency.

34. Law enforcement and independent investigations have determined that these schemes are perpetrated primarily in Southeast Asia, often via forced labor. Victims are trafficked into countries that include Myanmar, Philippines, Laos and Cambodia and are forced to conduct these scams via text messages, dating websites, and other online platforms inside scam compounds in these countries.[4]

35. In 2020—prior to the emergence of these types of scams—confidence schemes, or romance scams, were reported to have cost U.S. victims over $600 million dollars in losses. This represented a $125 million dollar increase from 2019, and $238 million dollars from 2018, for a total of $1.43 billion dollars in losses attributed to confidence schemes from 2018–2020. Separately, during this same time-period, investment scams were reported to have cost U.S. victims over $800 million dollars.[5]

36. Since the emergence of cryptocurrency-based confidence scams, those same scam

[3] dApps are decentralized applications on blockchain networks, and typically are run on smart contracts.

[4] Cezary Podkul and Cindy Liu, *Human Trafficking's Newest Abuse: Forcing Victims into Cyberscamming*, https://www.propublica.org/article/human-traffickers-force-victims-into-cyberscamming, (Sept. 13, 2022).

[5] Federal Bureau of Investigation Internet Crime Complaint Center, *Internet Crime Report 2020*, https://www.ic3.gov/AnnualReport/Reports/2020_ic3report.pdf, (Mar. 17, 2021).

categories have seen their losses multiply at significant levels, reaching a reported loss of over $5.22 billion dollars in 2023 alone for confidence schemes and investments scams combined.[6] And in 2024, that same loss increased to approximately $7 billion dollars.[7] In 2024 alone, approximately $5.8 billion in losses from cryptocurrency investment fraud was reported to the Internet Crime Complaint Center.[8]

37. One of the primary attributes of this type of scheme, which has helped further its success, is the use of smartphone applications. 97% of Americans own a cellphone of some kind and nine-in-ten own a smartphone.[9]

38. Among the seemingly endless list of smartphone applications ("apps") are mobile banking or investment apps, which are typically associated with an individual's bank or investment account. These apps typically display an account owner's balance and transaction history, among other information. Notably, as of 2022, nearly 80% of Americans regularly use mobile banking apps or websites.[10]

39. Generally, information contained within legitimate mobile banking or investment apps, such as the balance, history, and interest, can be assumed by the user to be accurate.

---

[6] Federal Bureau of Investigation Internet Computer Complaint Center, *Internet Crime Report 2023,* https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf, (Apr. 4, 2024).

[7] Federal Bureau of Investigation Internet Computer Complaint Center, *Internet Crime Report 2024,* https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf, (Apr. 23, 2025).

[8] *Id.*

[9] Eugenie Park, Kaitlyn Radde, Michelle Faverio, Olivia Sidoti, Risa Gelles-Watnick, Sara Atske and Wyatt Dawson, *Mobile Fact Sheet,* https://www.pewresearch.org/internet/fact-sheet/mobile/ (Nov. 13, 2024).

[10] American Bankers Association, *National Survey: Record Number of Bank Customers Use Mobile Apps More Than Any Other Channel to Manage Their Accounts,* https://www.aba.com/about-us/press-room/press-releases/consumer-survey-banking-methods-2024#:~:text=The%20national%20survey%20found%20that,in%20the%20past%2012%20months. (Nov. 22, 2024).

Furthermore, transactions performed on said legitimate app, reflected in the account history within the app, can generally be presumed to have occurred despite having no paper records like a receipt or statement one might receive if conducting the same transaction inside a brick-and-mortar institution.

40. This trust in mobile banking and investment apps is at the center of these schemes. Following the initial victimization through the confidence scheme, perpetrators convince victims to download what appear to be legitimate mobile banking or investment apps to track their cryptocurrency investments. In reality, they are not connected to any real account or legitimate financial institution. Instead, the apps are created and controlled by the perpetrators, who are able to create the facade of balances and transactions that are otherwise non-existent.

41. This fabricated activity, which on the surface would appear no different than that of a legitimate mobile banking or investment app, is made to appear as though investments into non-existent, perpetrator-controlled platforms are realizing substantial gains. This helps the perpetrators convince victims into investing additional funds into the scheme.

42. Victims may contribute a small amount of funds to a cryptocurrency confidence scam, unwittingly, only to see those funds triple in value, as displayed on the perpetrator-controlled app. After this point, some victims attempt to invest more assets, which may include IRAs, 401(k)s, home equity loans, and college savings plans.

43. Some victims report being able to successfully withdraw funds which establishes trust and credibility with the perpetrators. This stage in the fraud scheme is designed to give the victims more confidence to invest their remaining assets. In these scenarios, what actually happens is that victims likely withdraw funds deducted from their "investments" (rather than purported gains), or originating from other victims and not a legitimate investment opportunity. This

withdrawal ability deviates from more traditional confidence schemes and allows the scheme to continue for even longer.

44. Lastly, cryptocurrency confidence schemes most often involve cryptocurrency at the center of the investments. Cryptocurrency is well-known as a highly volatile asset, with price swings fluctuating the value of some cryptocurrencies, like Bitcoin, thousands of dollars in any given day. Cryptocurrency can also be highly technical, with terminology and attributes unique to different cryptocurrencies and blockchains. This has allowed for perpetrators to help convincingly explain convoluted investments to victims that otherwise would not consider purchasing or investing in cryptocurrency.

## STATEMENT OF FACTS

### Summary

45. OKX, a virtual currency exchange, contacted law enforcement officers regarding a large network of virtual currency accounts (the "144 OKX Accounts") they analyzed and believed were involved in receiving and transferring vast amounts of cryptocurrency scam proceeds—all controlled by a coordinated group of overseas actors. Law enforcement identified approximately 434 suspected fraud victims whose funds were likely laundered using this network. Law enforcement interviewed approximately 60 of those victims, who collectively lost approximately $19 million in cryptocurrency to scammers.

46. Investigators identified approximately 93 addresses to which victims deposited their virtual currency while under the belief that they were sending funds to legitimate exchange platforms (hereinafter, the "93 Initial Deposit Addresses"). Using the Last-in-First-Out ("LIFO")

tracing methodology,[11] victim funds from the 93 Initial Deposit Addresses with confirmed, identified victims' funds were sent to 22 of the 144 OKX Accounts after being cycled through a large set of "intermediary addresses," which law enforcement assesses were used by scammers for laundering purposes. Many of the intermediary addresses were themselves linked to even more cryptocurrency confidence scam victim reports containing multimillion dollar loss amounts.

47. Once victim funds were deposited to the 22 OKX accounts referenced above (the "22 OKX Accounts"), they were then laundered through many of the remaining 122 OKX accounts.[12] All 144 OKX Accounts are believed to be controlled by a group of cryptocurrency confidence scam actors and/or their money laundering co-conspirators. That assessment is based on their coordinated transaction activity, identical transaction counterparties, matching account naming conventions, similar know-your-customer information (including Vietnamese registrants and connections to ITECHNO[13]), and a list of overlapping identical IP addresses used by many of the 144 OKX Accounts, all of which have IPs tracing back to the Philippines.

48. Once the money launderers sent victim funds through the network of 144 OKX Accounts, they then laundered the funds even further through a group of 35 additional intermediary addresses, also likely controlled by the scammers and/or launderers. Funds traced through these 35 intermediary addresses ultimately were sent to the **SUBJECT VIRTUAL CURRENCY ADDRESSES**. On or about May 1, 2025, the Honorable United States Magistrate Judge Moxila A. Upadhyaya in the District of Columbia issued a seizure warrant for the approximately

[11] The LIFO method assumes that the first output back-traced was funded by the last input up to the amount of the original transaction deposited into one of the 144 OKX Accounts.

[12] Some of the 22 OKX accounts sent victim funds directly to intermediary addresses without first being laundered through the 122 remaining OKX accounts.

[13] *See infra* ¶¶ 61-63.

225,364,961 USDT associated with the **SUBJECT VIRTUAL CURRENCY ADDRESSES**.

49. This laundering involved hundreds of thousands of transactions. Due to the massive volume of transactions across a large network of addresses, this complaint describes the phases of laundering (including some specifics about relevant transactions) rather than detailing every single transaction.

**Origin of the Investigation**

50. In November 2023, the USSS San Francisco Field Office initiated an investigation into virtual currency accounts used to help launder funds derived from cryptocurrency confidence schemes. USSS received a report from Tether (which was working with OKX, a Seychelles-based virtual currency exchange) alleging that they identified approximately $250 million dollars in USDT traceable to cryptocurrency confidence scams that transferred through certain OKX accounts—which are included in the 144 OKX Accounts, as defined and further described below.

51. During the course of this investigation, law enforcement identified approximately 434 suspected cryptocurrency confidence scam victims, including 60 confirmed victims, whose funds can be traced to 22 of the 144 OKX Accounts, which the perpetrators controlled. Victim funds were not directly sent to the identified 144 OKX Accounts. Instead, the funds dissipated among various intermediary addresses before arriving in the 22 OKX Accounts, which were then generally cycled through the remaining 122 OKX accounts controlled by the same actors.[14] This is a common technique for laundering virtual currency fraud proceeds; the additional layering of transactions and continuous mixing of funds is a deliberate strategy to further obfuscate the true source of funds.

[14] The intermediary addresses themselves are exposed to, or have transacted with, even more fraud victim proceeds than were traceable to the OKX accounts.

52. This group of OKX Accounts then collectively transferred and consolidated funds into the **SUBJECT VIRTUAL CURRENCY ADDRESSES,** through an additional layer of intermediary addresses, which is consistent with concealment money laundering.

**OKX Accounts**

53. Among the details provided by OKX and Tether in their initial report to USSS was the existence of the 144 OKX Accounts that appeared to be involved in linked activity, sharing elements such as exact IP addresses used by the accounts, transaction counterparties, and photographic traits in know-your-customer ("KYC") information. This indicates that the 144 OKX Accounts are all likely controlled by the same organized entity and interconnected for laundering purposes. As stated earlier and further described below, 22 of the 144 OKX Accounts are confirmed to have received cryptocurrency confidence scam victims' virtual currency, while the other accounts are believed to have been used to further launder the currency within the group's network while the group-maintained control of the funds.

54. Specifically, nearly all of the 144 OKX Accounts were accessed via IP addresses in the Philippines, and all were associated with email addresses using a specific and easily identifiable naming convention—iCloud emails that featured seemingly random letters followed by the user's phone number, such as the following:

| *Name* | *Phone* | *Email* |
|---|---|---|
| *LE CONG DAT* | *9603183083* | *dbr9603183083@icloud.com* |
| *TIEN LY TIEN LY* | *9603183097* | *nabi9603183097@icloud.com* |
| *NGUYEN MINH THANH* | *9696354341* | *c9696354341@icloud.com* |

55. The 144 OKX Accounts were all opened using Vietnamese identification documents and KYC photos that, based on the background and identifiable items such as cameras and artwork, appear to be taken in the same location. This an indicator that the accounts are controlled by individuals working in a "scam compound," or a location operating for the sole purpose of perpetrating cryptocurrency confidence scams and laundering proceeds.[15]

56. Additionally, the 144 OKX Accounts all received and sent funds to the same addresses. According to the Financial Action Task Force (FATF),[16] frequent transfers to or from the same transaction counterparties by more than one person from the same IP address is a red flag indicator of money laundering.[17] This is used as a laundering technique to develop circular transactions that complicate tracing but keep the funds within a set universe of virtual currency addresses.

57. Virtual currency transactions involving accounts that send and receive funds from the same counterparties using overlapping IP addresses can indicate concealment money laundering by obscuring the origin and destination of funds through multiple transactions without a legitimate business purpose. This indicates that the 144 OKX Accounts often transacted with the

[15] A scam compound is a location where workers, often victims of human trafficking themselves, work in conjunction to defraud victims and launder victim funds.

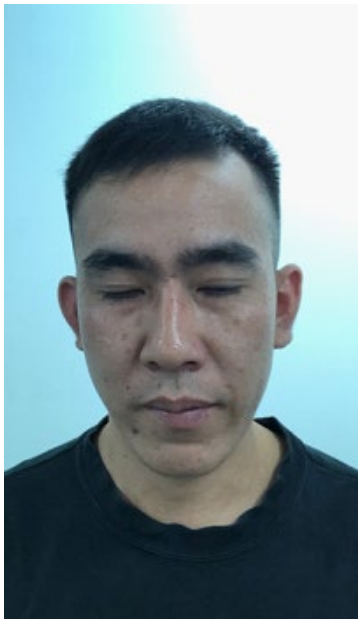
[16] FATF is "the global money laundering and terrorist financing watchdog. It sets international standards that aim to prevent these illegal activities and the harm they cause to society." The Financial Action Task Force, *Our Topics,* https://www.fatf-gafi.org/ (Last accessed Jun. 17, 2025).

[17] According to a report released by FATF in September 2020 on Virtual Assets (VA) Red Flag Indicators of Money Laundering (ML) and Terrorist Financing (TF), one of the red flag indicators related to transaction patterns includes making frequent transfers in a certain period of time to the same virtual asset (VA) account by more than one person; from the same IP address by one or more persons; or concerning large amounts.

The Financial Action Task Force, *FATF REPORT Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing* https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-Red-Flag-Indicators.pdf.coredownload.pdf (Sept. 2020).

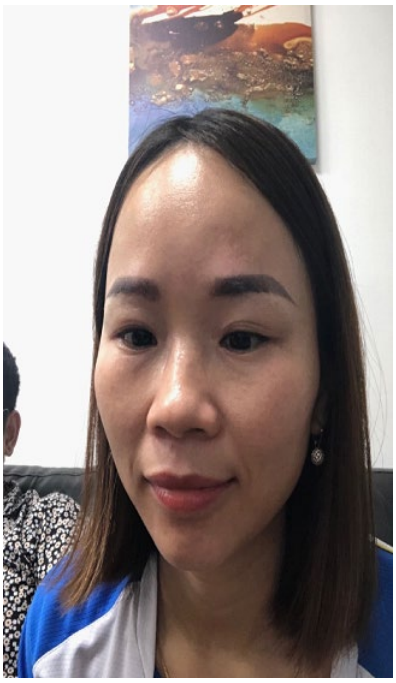
same intermediary addresses used to launder stolen funds. This pattern suggests a single control point attempting to mask the true source and ownership of the money, which is often seen in layering and circular transactions designed to complicate virtual currency tracing. The lack of geographic diversity and economic justification of these transactions, which accumulate fees, combined with the questionable KYC information, further points to efforts to conceal the illicit nature of the funds.

58. Rather than a "selfie" style photo, which is more common for KYC photos, the KYC photos for the 144 OKX Accounts appear to be taken by a separate individual. Examples highlighting the likelihood of a separate photographer are depicted below:


59. In other instances, the KYC photos reveal that the account owners appear to be located in the same facility, which may be a call center or scam compound. And in several cases, they are seated next to each other. This is indicative of "mule" accounts established to help facilitate the receipt and laundering of fraud funds. An example of KYC photos that appear to be taken in the same location is depicted below. Specifically, two separate account owners are seated next to each other with the same painting in the background. The two accounts associated with

these photos, which are among the 144 OKX Accounts, were used to receive large volumes of funds believed to be associated with cryptocurrency confidence schemes, among potentially other types of crimes.



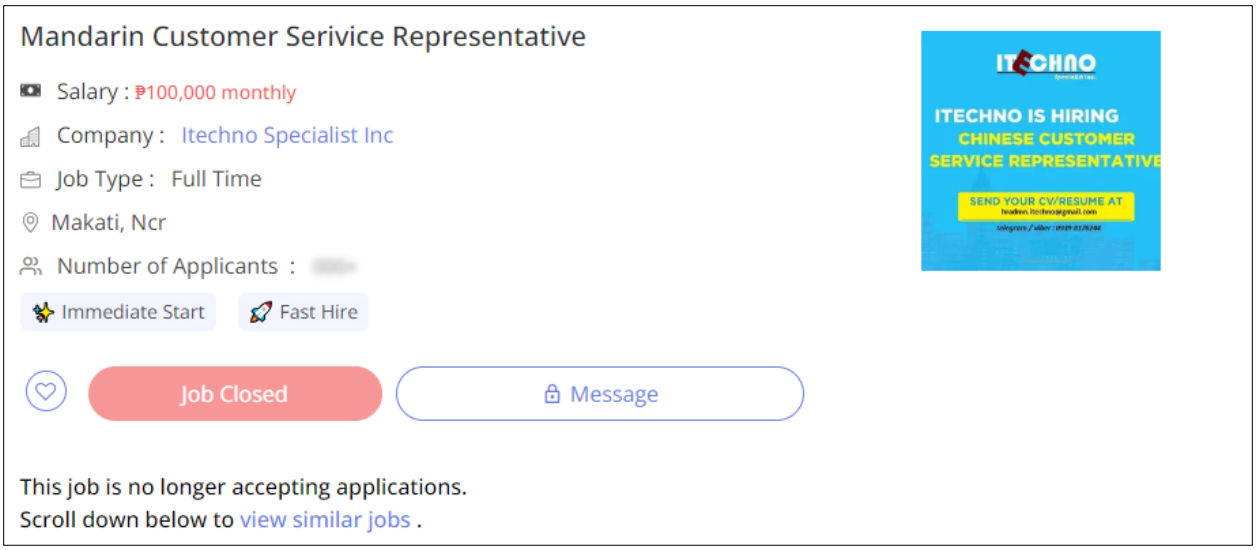
60. In at least two of the 144 OKX Accounts, accounts were listed under the same individual, utilizing the same ID card with identical identifiers but two separate KYC photos.

61. Additionally, in at least two instances, OKX Accounts were associated with KYC photos depicting individuals holding or wearing a lanyard with the business name "ITECHNO Specialist Inc," which is depicted below:[18]


62. Law enforcement has determined that ITECHNO Specialist Inc was a call center located in Manila, Philippines.[19] Law enforcement located several job postings seeking applicants, including the advertisement depicted below:

[18] The "E" in ITECHNO is printed in a darker color that blends in with the lanyard.

[19] It is currently unclear whether ITECHNO is still in existence or has changed its name and location.




63. The advertisement depicted above seeks Mandarin speaking customer service representatives. It goes on to further state, "Powerful enterprise. We are recruiting a large number of customer service staff, both men and women…" and "…traveling to the Philippines from other countries, the company will bear the entire cost. Travel expenses are fully deductible after 3 months of employment." This description is consistent with the forced-labor call centers known to facilitate cryptocurrency confidence schemes.[20] This also helps explain why each of the 144 OKX Accounts, including the 22 OKX Accounts receiving funds traceable to known victims, was opened with Vietnamese KYC documents but used IP addresses in the Philippines. The use of Vietnamese KYC documents for the 144 OKX accounts connecting through Philippine-based IP addresses are consistent with foreign labor being used in cryptocurrency confidence scam compounds.

64. An analysis of the IP addresses associated with logins to the 144 OKX Accounts revealed overlap in IP addresses, further linking them to the custody and control of a coordinated group. Specifically, 132 of the 144 OKX Accounts were accessed by at least one IP address that accessed two or more other OKX accounts within the group of the 144 OKX Accounts. In several instances, a single

[20] *See supra* note 4.

IP address was linked to as many as five separate OKX Accounts (out of the 144 OKX Accounts), such as 175.176.40.136. Nearly all of these IP addresses resolved to domain hosting providers in the Philippines. According to the previously mentioned FATF Red Flag Indicators of Money Laundering report, a red flag indicator related to anonymity includes a large number of seemingly unrelated accounts controlled from the same IP address.[21] In this instance, several accounts using the same IP addresses, receiving fraud proceeds from the same schemes, opened with overlapping or suspicious Vietnamese KYC information, demonstrate that the 144 OKX Accounts are interconnected in the money laundering scheme.

65. Law enforcement analyzed the transactional activity associated with the 144 OKX Accounts and observed over *263,000 deposit transactions* that cumulatively totaled about *three billion dollars* in transactions. Notably, 98% of these transactions were conducted between November 2022 and November 2023. Within that one-year period, the 144 OKX Accounts involved in laundering victim funds engaged in approximately 257,740 transactions, involving virtual currency worth approximately $2,940,000,000. This creates an average of over 700 transactions moving more than $8 million per day during this isolated one-year period.

66. The combination of factors including the common Vietnamese KYC information used to open these accounts that are almost exclusively accessed from the Philippines, the common transaction counterparties, the shared and overlapping IP addresses, the suspicious and connected KYC photographs, the ITECHNO job posting, the sheer amount of transactions—approximately 263,000 over their lifespan,

[21] According to the previously mentioned FATF VA Red Flag Indicators of ML and TF report, a red flag indicator related to anonymity includes a large number of seemingly unrelated virtual asset wallets controlled from the same IP-address (or MAC-address), which may involve the use of shell wallets registered to different users to conceal their relation to each other.

The Financial Action Task Force, *FATF REPORT Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing* https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-Red-Flag-Indicators.pdf.coredownload.pdf (Sept. 2020).

and funds passing through the related 144 OKX Accounts—approximately $2,940,000,000—indicate that these accounts were used for high-volume money laundering.

**Victim Identification**

67. In reviewing and tracing virtual currency in and out of these accounts, law enforcement utilized the LIFO method of accounting, which assumes that the first output back-traced was funded by the last input up to the amount of the original transaction deposited into one of the 144 OKX Accounts.

68. Among the deposit transactions, law enforcement was able to identify over 1,200 transactions where, based on interviews in this investigation, individuals believed to be scam victims sent funds from virtual currency exchanges to addresses identified as part of the LIFO tracing. These transactions were sent by approximately 434 individuals (believed to be victims of cryptocurrency confidence scams, as identified based on interviews described below) located primarily in the U.S., but also from the UK, Australia, and Germany. The victims ultimately sent over $19 million dollars to virtual currency addresses at the direction of scammers. After being laundered through intermediary addresses, portions of that $19 million arrived in the 22 OKX Accounts identified above.

69. Despite the large transaction count (i.e., 1,200 transactions), the funds (approximately $19 million) were initially sent by victims to only 93 different virtual currency addresses, which can be typical of cryptocurrency confidence schemes where suspect-controlled scam addresses are used to receive funds from multiple victims. These 93 different virtual currency addresses represent the addresses scammers provided the victims, either directly or through scam websites, as the deposit address for their virtual currency "investments".

70. These 93 Initial Deposit Addresses were further analyzed and determined to have collectively received over $62 million dollars. Suspected victim transactions to the 93 Initial Deposit Addresses are believed to have started as early as on or about March 17, 2022. Addresses used in the

initial receipt of cryptocurrency confidence scam proceeds are likely to be utilized solely for the purpose of receiving such funds, and likely all approximately $62 million dollars' worth of virtual currency deposited into those 93 Initial Deposit Addresses represents proceeds from additional cryptocurrency confidence victims. In part, this is because those operating such fraud schemes do so full-time and therefore do not have any significant alternative source of legitimate virtual currency income to send to such deposit addresses. Moreover, combining legitimate with illegitimate income could create operational risks for the operators of such fraud schemes as legitimate accounts might be subject to scrutiny by those not involved in the offense conduct, such as accountants and staff at legitimate banks and virtual currency exchanges. Furthermore, in the course of their investigation, law enforcement has not found a witness who deposited funds into the 93 Initial Deposit Addresses for legitimate purposes.

71. USSS performed outreach to the individuals identified as senders to the Initial Deposit Addresses identified by the back-tracing. As explained above, of the approximately 434 individuals believed to be victims of cryptocurrency confidence scams, as identified based on interviews described below, law enforcement successfully contacted 60 individuals[22] and learned that in all but one instance, the individual reported being the victim of a cryptocurrency confidence scam. In addition to the 60 individuals interviewed, law enforcement also located 42 victim reports on complaint databases, including the FBI's Internet Crime Complaint Center ("IC3") and Federal Trade Commission's ("FTC") Consumer Sentinel systems, detailing cryptocurrency confidence scams that referenced some of the 93 Initial Deposit Addresses.[23]

[22] Law enforcement received no response or was unable to reach the remaining victims. Victims of cryptocurrency confidence scams are often reluctant to respond to outreach for fear that they are being victimized once again. Indeed, in some scams, the perpetrators attempt to re-victimize existing victims by posing as government authorities and then seeking financial payments/fees purportedly (but fraudulently) represented as needed to secure the return of previously stolen funds.

[23] Some of these victim reports were submitted by victims counted among the 60 confirmed, interviewed victims.

72. Based on these determinations and the totality of the circumstances, the evidence suggests all of the remaining funds that passed through the 93 Initial Deposit Addresses are funds tied to cryptocurrency confidence scam victims.

73. The investigative team was able to back-trace victim funds from the 22 OKX Accounts (among the 144 OKX Accounts) using LIFO. This is believed to represent a sampling of the overall activity, which features total transactions in excess of 263,000 deposits.[24]

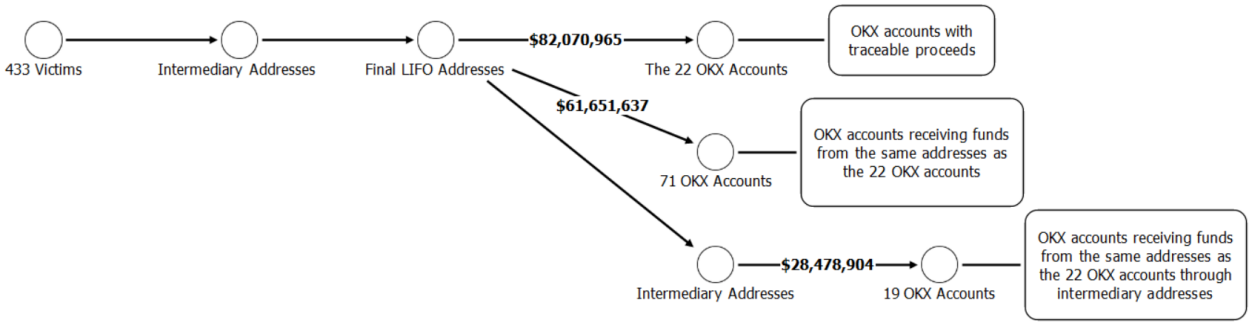
74. Further analysis of the remaining 122 OKX accounts determined that they received funds directly and indirectly from many of the same addresses that directly transacted with the 22 OKX Accounts.

75. Law enforcement determined that 71 of the 144 OKX Accounts received over approximately $61 million dollars from the same addresses identified in the LIFO back-tracing as having sent cryptocurrency confidence scam proceeds to the 22 OKX accounts.

76. Additionally, another 19 OKX accounts similarly received funds that passed through the same addresses identified in the LIFO back-tracing through numerous additional intermediary addresses. This activity is illustrated below; all values are approximate:[25]

[24] The extraordinarily large volume of transactions involved in this case complicates cryptocurrency tracing efforts, however, USSS deployed a strategic tracing session and methodology involving over a dozen USSS personnel from throughout the country that helped identify large volumes of victims and fraud traceable to the 144 OKX Accounts during a week-long law enforcement operation in Northern California.

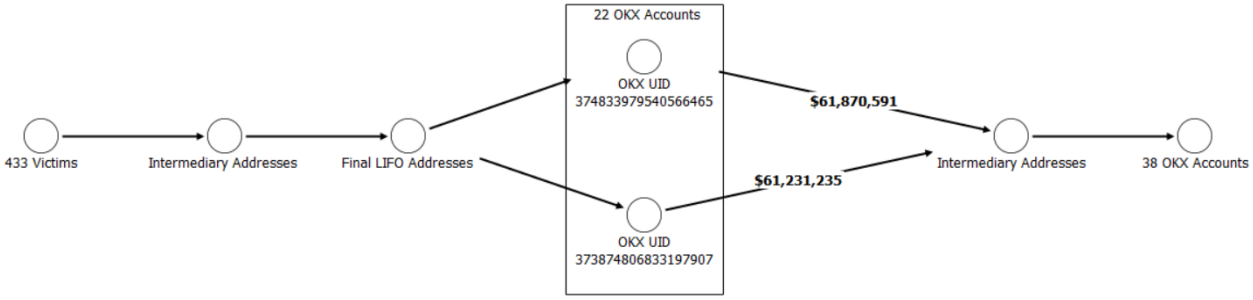
[25] For the purpose of the chart on this page, "Final LIFO Addresses" references the counterparty addresses directly sending known victim funds to the 22 OKX Accounts.




77. Actors involved in the laundering of proceeds from scams such as cryptocurrency confidence schemes do not typically commingle clean funds with stolen funds outside of the purpose of further laundering the cryptocurrency confidence scam funds. Therefore, the funds received from the same intermediary addresses likely consist of the proceeds of cryptocurrency confidence scams, or similar scams, and are commingled for the purpose of concealing, disguising, and laundering the funds.

78. Law enforcement observed that many of the 144 OKX Accounts, which are not all referenced in the above illustration, did not in fact receive funds directly traceable through LIFO analysis to cryptocurrency confidence scam victims in the same manner detailed above. Rather, they received funds through other OKX accounts that acted as pass-through accounts.

79. For example, two OKX accounts, which are part of the 22 OKX Accounts that law enforcement identified as receiving proceeds traceable to cryptocurrency confidence scams, sent their funds to numerous intermediary addresses that ultimately redeposited those funds into 38 of the 144 OKX Accounts not already referenced in the illustration above. These are transactions that serve no legitimate business purpose because each transaction incurs fees. These two OKX accounts represent one example of the cyclical activity observed within the 144 OKX Accounts that appears to have been conducted to obfuscate the true source of funds. The activity referenced above is illustrated below; values are approximate:




80. For each of the 22 OKX Accounts with traceable scam proceeds, law enforcement observed numerous instances where funds were sent from the victim's initial account at a virtual currency exchange to a suspect address (the 93 Initial Deposit Addresses). The funds were then sent through numerous transactions in rapid succession in what appears to be an effort to obfuscate the nature, source, control, and/or ownership of those proceeds, before they were ultimately deposited at one of the 22 OKX accounts.

81. Sending virtual currency to several addresses in rapid succession can be evidence of concealment money laundering as it suggests an attempt to obfuscate the origin and flow of funds through a process known as "layering." This technique involves quickly moving funds through multiple addresses to create a complex web of transactions, making it difficult for investigators to trace the money back to its source. The rapid, fragmented distribution of funds can mask the overall transaction patterns and hinder the identification of the original illicit activity, thereby concealing the true ownership and origin of the money. Transferring virtual currency between several addresses in rapid succession is likely not for a legitimate business purpose because each transaction accumulates fees, and the owner therefore loses money with each transfer.

**Cryptocurrency Confidence Scam Victim Reports**

82. As previously mentioned, law enforcement's victim identification efforts located approximately 434 suspected victims of cryptocurrency confidence scams involving common money laundering transactions. These victims sent approximately $19 million dollars to addresses (i.e., the 93

Initial Deposit Addresses) whose funds were ultimately received by the 22 OKX Accounts. These 93 Initial Deposit Addresses received over $62 million dollars. Initial deposit addresses that scammers provide to victims are typically exclusively used to receive and transfer victim proceeds rather than also being used for licit transactions. This is because when many victims realize they have been scammed, many report to law enforcement. Victims often provide the deposit address(es) where they sent their virtual currency, which exposes these addresses to law enforcement scrutiny and invites potential for freezes and seizures. Therefore, the funds sent to and from the 93 Initial Deposit Addresses likely originate from additional, unidentified victims of cryptocurrency confidence or related scams. These victim totals are believed to represent just a portion of the true magnitude of the scheme.

83. The victim funds were funneled through hundreds of intermediary addresses, starting with the 93 Initial Deposit Addresses, then moving through intermediary addresses to the 22 OKX Accounts, then through many of the remaining 122 OKX accounts (among the 144 OKX Accounts), and eventually into the **SUBJECT VIRTUAL CURRENCY ADDRESSES**.

84. Because of the sheer volume of transactions and complex web of intermediary addresses, tracing a single victim deposit all the way through to the **SUBJECT VIRTUAL CURRENCY ADDRESSES** is incredibly time consuming for even a team of investigators. With hundreds of high-frequency transactions designed to complicate tracing efforts, it is also difficult to determine which outgoing transaction involves each specific input of fraud victim funds. Nonetheless, below are a few examples of the tracing from start to finish, showing the strategy employed to obfuscate and conceal transactions by intermingling traced victim funds with additional funds of unknown origins.

85. **S.H. in Elkhart, KS.** Among the list of victims whose funds are traceable to one or more of the 22 OKX Accounts was S.H., formerly the CEO of Heartland Tri-State Bank in Elkhart, Kansas who embezzled bank funds to invest on a virtual currency platform that turned out to be part of a

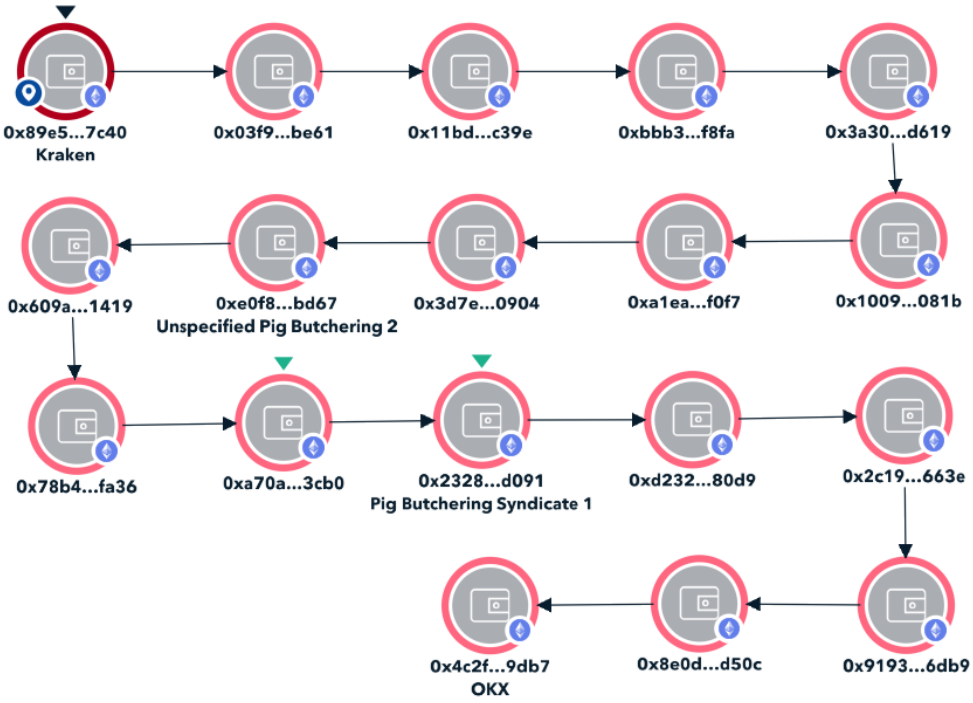
cryptocurrency confidence scam. In February 2024, S.H. was charged in the District of Kansas with bank embezzlement for the theft of approximately $47.1 million dollars from the bank's assets, and was later sentenced to 293 months in prison after pleading guilty.[26] According to a report released by the Federal Reserve Board ("FRB"), Hanes embezzled nearly $50 million dollars in order to conduct wire transfers as part of a cryptocurrency confidence scheme.[27] That is, Hanes was both perpetrator (embezzling funds from the bank) and victim (to invest those funds in virtual currency as directed by subjects perpetrating a cryptocurrency confidence scheme against him whereby they defrauded him of those embezzled funds).

86. S.H.'s funds were back-traced beginning at one of the 22 OKX Accounts whose deposit address begins with 0x4c2f. This account received 11 deposits on or about August 14, 2023, totaling approximately 197,597 USDT.[28] These funds were back-traced using the LIFO method through 17 transactions, or "hops," to Kraken, a U.S.-based virtual currency exchange. Records reviewed from Kraken identified S.H. as sending 3,116,350 USDT from his Kraken account on or about June 28, 2023, to one of the 93 Initial Deposit Address (beginning with 0x03f9). An illustration of this flow of funds is provided below:

[26] United States Attorney's Office District of Kansas, *Former CEO of Failed Bank Sentenced to Prison,* https://www.justice.gov/usao-ks/pr/former-ceo-failed-bank-sentenced-prison, (Aug. 19, 2024).

[27] Board of Governors of the Federal Reserve System, *Material Loss Review of Heartland Tri-State Bank,* https://oig.federalreserve.gov/reports/board-material-loss-review-heartland-tri-state-bank-feb2024.pdf (Feb. 7, 2024).

[28] 1 USDT is the equivalent to 1 US Dollar.




87. This transaction from S.H. to the 0x03f9 initial deposit address is consistent with FRB's report of the Heartland Tri-State Bank failure, which detailed a $3.3 million dollar wire transfer on June 27, 2023, from Heartland Tri-State Bank's assets. As depicted above, Hanes's initial virtual currency deposit into the fraud scheme was $3.3 million dollars. It was transferred through 16 wallet addresses before it arrived at the OKX exchange in one of the 22 OKX Accounts receiving illicit criminal proceeds. Through exchange fees, laundering techniques, and peel chain-type movement,[29] the final amount of victim funds to arrive at the 0x4c2f OKX address was less than the initial $3.3 million. This address is connected to the **SUBJECT VIRTUAL CURRENCY ADDRESSES** because its associated OKX account sent approximately $6 million in virtual currency to three intermediary addresses, one of which

[29] A peel chain is a technique used to launder a large amount of virtual currency through a lengthy series of minor transactions. It occurs when virtual currency sitting at one address is sent through a series of transactions in which a slightly smaller amount of virtual currency is transferred to a new address each time. In each transaction, some quantity of virtual currency "peels off" the chain to another address (frequently, to be deposited into a virtual currency exchange), and the remaining balance is transferred to the next address in the peel chain.

then transferred its funds to two of the **SUBJECT VIRTUAL CURRENCY ADDRESSES, USDT Token Group A, and B**.

88. **M.S. in La Vernia, TX.** Another OKX account (i.e., one of the 22 OKX Accounts), whose deposit address begins with 0x2bef, was back-traced using the LIFO method to a victim in La Vernia, Texas. This OKX account received twelve deposits on or about May 22, 2023, totaling approximately 116,334 USDT. These funds were back-traced using the LIFO method through eleven transactions, or hops, to Coinbase, another U.S.-based virtual currency exchange. Records reviewed from Coinbase identified the sender as M.S. Law enforcement interviewed M.S. and determined that M.S. was a cryptocurrency confidence scam victim who sent funds to one of the 93 Initial Deposit Addresses beginning with 0x414f ("0x414f ")[30] as part of a cryptocurrency confidence scam.

89. Notably, the 0x414f address is a significant cryptocurrency confidence scam address, having received nearly $3.6 million dollars in cryptocurrency. Law enforcement identified 39 individuals who sent funds to this address. USSS has interviewed many of these individuals (counted among the approximately 60 total victims interviewed), and the interviews along with IC3 and FTC complaints show that this address has been used extensively for cryptocurrency confidence schemes.

90. **Additional Victim Examples.** Additional victims who reported transferring virtual currency to 0x414f include the following:[31]

91. On February 29, 2024, a USSS Special Agent interviewed M.L., a victim who resides in Phoenix, AZ. M.L. stated that in or around May 2023, he met an unknown woman on LinkedIn. M.L. stated that he was quickly instructed by the female to continue conversation via encrypted mobile

[30] 0x414f61e4057ea79279e4970cfdad198ebe70092b

[31] This list is not an exhaustive compilation of victim interviews conducted and represents a sampling of the victims interviewed thus far.

applications WhatsApp and Telegram. M.L. said that he was subsequently introduced to virtual currency investment by the female and promised significant investment returns on his money. Typically, cryptocurrency confidence scams guarantee an unrealistic return on investment. M.L. stated that the female sent him a link to "FX6," and he was instructed to click on the link and access the "investment platform." M.L. sent funds to 0x414f believing that he was investing in a legitimate platform. M.L. stated that he was able to withdraw $500 from his investment platform into his bank account. However, M.L. stated that he was unable to withdraw additional funds from the platform and was subsequently locked out of his account. M.L. reported losing $50,000 to the scam.

92. On or about March 18, 2024, USSS Special Agents interviewed D.M., who resides in Alexandria, VA. D.M. reported that in approximately May 2023, he received a text message from an unknown number. D.M. stated that an unknown subject identified herself as "Anne." D.M reported that Anne asked him to communicate via WhatsApp. D.M. stated that the subject was in the financial industry and had offered to demonstrate trading virtual currency via "FX6 Pro." The unknown subject eventually convinced D.M. to download an app called AI TradeMateFX6Pro from the Apple Store. D.M. invested $485,000 in virtual currency and reported receiving specific instruction for every transfer he conducted. D.M. sent funds to 0x414f believing that he was using a legitimate platform. When D.M. attempted to withdraw his funds from the platform, he was told he needed to pay the "taxes"[32] on his earning. D.M. reported paying "taxes," however he was told that he also needed to pay a late fee. D.M. stated that he

[32] Cryptocurrency confidence scammers often allow victims to withdraw large sums of money, to boost their confidence in the investment scheme.

*See* Ken Dilanian, *With 'pig butchering' scams on the rise, FBI moves to stop the bleeding,* https://www.nbcnews.com/news/crime-courts/pig-butchering-scams-rise-fbi-moves-stop-bleeding-rcna137009, (Feb. 5, 2024).

paid $63,000 for the late fee. D.M. stated that after paying the fee, he was still unable to withdraw his funds from the platform and he reported losing $548,000 to the scam.

93. According to the FBI's IC3, on or about March 3, 2024, a report was filed by R.M. R.M. is a cryptocurrency confidence scam victim, who resides in Ankeny, Iowa. R.M. reported being contacted by "Yunski Tang" on LinkedIn. R.M. reported that Tang described herself as a young Chinese professional woman who was working in the U.S. R.M reported that Tang was looking for an experienced mentor to help her understand American culture and asked R.M to communicate via WhatsApp. R.M. reported that Tang then introduced him to virtual currency and subsequently convinced him to start investing in the Bitdu platform. R.M. sent funds to 0x414f believing that he was investing in a legitimate platform. R.M. observed what he believed to be a large financial gain on his initial transaction. R.M. reported successfully withdrawing a few thousand dollars from his "investment account." R.M. stated that Tang told him that she had an intelligent uncle in San Francisco who knew the market. When R.M. attempted to withdraw his funds from the platform but was told by Tang that he needed to deposit investment taxes in the Bitdu Tax account or he would be charged with a federal crime of avoiding taxes. R.M. reported losing contact with Tang and was unable to access the Bitdu website or the investment platform. R.M reported losing $11,000 to the scam.

94. **T.D. in Laguna Beach, CA.** In another instance, USDT deposits to one of the 22 OKX Accounts, whose deposit address begins with 0x4c2fb, were back-traced using the LIFO method to T.D., a victim in Laguna Beach, California. Records reviewed from Kraken identified the victim as T.D., who transferred nearly $50,000 to one of the Initial Deposit Addresses, which begins with 0x2b7c7. On or about February 28, 2024, a USSS Special Agent interviewed T.D. T.D. stated that he was unaware that he was a victim of a virtual currency scam. T.D. stated that a Chinese male, who identified himself as Jason Liu Qiang, approached him during a real estate open house he was showing. T.D. stated that Qiang

introduced himself as a virtual currency trader and offered T.D. an opportunity to invest in YoBitPro.lol. T.D. stated that Qiang quickly suggested that they communicate via WhatsApp. T.D. stated that Qiang promised significant financial return for his investments and matched the amount of deposit into T.D.'s platform account. T.D. reported transferring $250,000 into the platform and having over $1,200,000 in profits. T.D. advised that he never attempted to withdraw any funds from the platform and did not think it was suspicious. The Special Agent who interviewed T.D. advised T.D. that the investment platform is a scam and to cease all payments and communication with Qiang. On March 5, 2024, USSS Special Agents interviewed T.D. at his residence. T.D. advised that he attempted to withdraw his funds from the investment platform and was asked to pay the "withdrawal taxes bill." T.D. shared that he paid $50,000 for the fee and was still unable to withdraw the funds. T.D. was advised to not pay any additional fees and cease all communication with Qiang.

95. **M.C. in Dallas, TX.** Among the 22 OKX Accounts described in paragraphs above was an account with a deposit address beginning with 0x029b, which was back-traced using the LIFO method to M.C., a victim in Dallas, Texas. Records received from the virtual currency exchange Crypto.com identified the victim as M.C., who transferred cryptocurrency worth over $420,000 to one of the 93 Initial Deposit Addresses, which begins with 37HmBH. On February 29, 2024, a USSS Special Agent interviewed M.C. M.C. stated that one year ago he was contacted by a female named Sophia via mobile App "Salams." M.C. stated that she immediately started to talk about virtual currency investment with guaranteed financial returns. M.C. was provided a link by Sophia to a website "digfntz.com" to access the investment platform. M.C. reports investing $1,900,000 into the platform. M.C. states that when he attempted to withdraw his funds from the platform, he was asked to pay significant withdrawal fees. M.C. stated that he refused to pay the fees and realized that he was scammed. M.C. stated that his account

balance with the investment platform was approximately $7,000,000. M.C. stated that he stopped communicating with Sophia and subsequently lost access to his investment account.

96. These narratives are representative of similar stories told by all 60 victims interviewed by law enforcement, as well as the IC3 and FTC reports referenced above, including for victims that were not interviewed by law enforcement.

97. Law enforcement personnel tracing the funds into the 22 OKX Accounts observed multiple instances where different behaviors indicated efforts to obfuscate the source or destination of funds. This included instances of chain hopping, where funds were sent from one blockchain to another, sometimes swapping the type of cryptocurrency, like BTC to USDT. This activity breaks the pathway on the blockchain for the funds and makes them more difficult to trace. Other behaviors include the rapid movement of funds, with many tracings featuring transactions occurring within minutes of each other over multiple hops. This pattern of activity was repeatedly noted during the tracing efforts and is an indication of concealment money laundering. The remaining transactions and activity likely derive from cryptocurrency confidence schemes and other similar scams.

**Intermediary Addresses Used to Launder Funds**

98. As discussed above, the typical pattern of fraud and laundering involved victims transferring their "investment" funds into one of the 93 Initial Deposit Addresses. The criminal actors then laundered the funds through several intermediary addresses before being consolidated into the 22 OKX accounts. In some instances, there were as few as eight intermediary addresses between the 93 Initial Deposit Addresses and one of the 22 OKX Accounts, while in others, there were nearly 100 intermediary addresses. Law enforcement performed additional analysis on the intermediary addresses and discovered that these intermediary addresses were listed in additional cryptocurrency confidence scam victim complaints as being involved in hundreds of millions more in victim losses. At times, the

intermediary addresses were listed as initial deposit addresses for additional cryptocurrency confidence scam victims. At other times, investigators noticed intermediary addresses were used by scam operators to launder funds believed to be from additional victims (outside of the victims identified in this investigation) after those victims made their initial deposits.

99. Simply put, not only were the 93 Initial Deposit Addresses linked to extensive amounts of cryptocurrency confidence scam fraud, but so were the intermediary addresses that they sent funds to, some of which also directly received cryptocurrency confidence scam proceeds from victims. The presence of numerous victims of similar fraud is a likely indication that the intermediary addresses involved were also used in the laundering of funds tied to cryptocurrency confidence scams, among potentially other types of fraud, and that the funds received by the 22 OKX Accounts are either the proceeds of a specified unlawful activity, to wit, wire fraud, directly traced to victims, or other funds of unknown specific origins that, based on their transaction history patterns, are also believed to have been involved in concealment money laundering.

100. The intermediary addresses themselves are listed in IC3 and FTC complaints as addresses receiving approximately $68 million in cryptocurrency confidence scam victim funds in addition to the $62 million received by the 93 Initial Deposit Addresses described previously. These are funds that were then commingled in the laundering process with identified victims' funds who deposited their virtual currency into the 93 Initial Deposit Addresses.

101. The following sections describe—for each of the above-referenced 22 OKX Accounts receiving victim funds (which are part of the 144 OKX Accounts controlled by the same perpetrators)—the tracing conducted by law enforcement, which shows the amount of fraud proceeds related to each of those 22 OKX Accounts, as well as how the criminal actors used the intermediary addresses to launder the funds before depositing them into the 22 OKX Accounts. In summary, the

identified 22 OKX Accounts received fraud funds not only from the victims identified in this investigation, but also from additional individuals believed to be victims who deposited their money in some of the intermediary addresses identified in this investigation. These funds were combined in the 22 OKX accounts, and then further laundered through the other 122 OKX accounts and additional intermediary addresses before some of the funds eventually were transferred into the **SUBJECT VIRTUAL CURRENCY ADDRESSES.**

**OKX ACCOUNT USER ID 374833979540566465[33]**

102. Law enforcement back-traced funds from OKX account 374833979540566465 ("6465") and identified 14 intermediary addresses between the Initial Deposit Addresses and 6465's deposit address. These 14 addresses were used to launder proceeds traceable to additional cryptocurrency confidence scams. Law enforcement located four IC3 cryptocurrency confidence scam victim reports that reference three of the 14 intermediary addresses. The victim reports list a combined loss amount of approximately $958,355.78. The presence of funds from multiple victims of similar fraud schemes within the same network of addresses is a likely indication that the addresses are involved in the laundering of fraudulently obtained funds. These addresses, used as intermediary addresses, as well as initial deposit addresses for IC3 complainants, transferred funds to this 6465, including wire fraud proceeds, as part of the launderers' scheme to use 6465to conceal or disguise the proceeds.

103. The three intermediary addresses referenced in the IC3 reports, which reported just below $1,000,000 in fraud losses, have cumulatively received nearly $74 million dollars' worth of virtual currency. Typically, addresses used to initially receive criminal proceeds in cryptocurrency confidence

[33] In paragraphs 102-187, "Initial Deposit Address" and "Initial Deposit Addresses" refer to virtual currency addresses within the 93 Initial Deposit Addresses that are displayed in the tracing exhibit accompanying the examples for each of the respective 22 OKX Accounts.

scams are likely to be utilized solely for the purpose of receiving such funds or otherwise involved in the laundering of such funds to help further obfuscate the source, control, ownership, and destination of funds.

104. This pattern of activity is illustrated in Exhibit 1.[34]

**OKX ACCOUNT USER ID 389805680867066989**

105. Law enforcement back-traced funds from OKX account 389805680867066989 "6989" and identified 20 intermediary addresses between the Initial Deposit Address and 6989's deposit address. These 20 addresses were used to launder proceeds traceable to cryptocurrency confidence scams. Law enforcement located three cryptocurrency confidence scam IC3 reports that reference four of the 20 addresses. According to the IC3 reports, these addresses are tied to approximately $2,411,885 in victim funds.

106. While the four addresses are associated with nearly $2.5 million in losses, they cumulatively received over $124 million dollars in cryptocurrency. Typically, addresses used to initially receive criminal proceeds in cryptocurrency confidence scams are likely to be utilized solely for the purpose of receiving such funds or meant to be involved in the laundering of such funds to help further obfuscate the source, control, ownership, and destination of funds.

107. This pattern of activity is illustrated in Exhibit 2 showing the series of hops for no legitimate purpose, and the varied placement of the IC3-reported addresses (denoted in red) in the laundering chain, used as both initial victim deposit addresses and intermediary addresses for further concealment.

[34] Addresses with victim reports denoted in red.

**OKX ACCOUNT USER ID 384075896514085732**

108. Law enforcement back-traced funds from OKX account 384075896514085732 ("5732") and identified 36 intermediary addresses between the Initial Deposit Addresses and 5732's deposit address. Law enforcement located 25 cryptocurrency confidence scam IC3 reports that reference six of the 36 addresses as being involved in cryptocurrency confidence scam losses totaling approximately $11,714,891.38.

109. These six addresses referenced in IC3 reports have cumulatively received over $240 million dollars in virtual currency. Typically, addresses used to initially receive criminal proceeds in cryptocurrency confidence scams are likely to be utilized solely for the purpose of receiving such funds or meant to be involved in the laundering of such funds to help further obfuscate the source, control, ownership, and destination of funds.

110. This pattern of activity is illustrated in Exhibit 3, showing a series of transactions with varying numbers of hops for no legitimate purpose between initial victim deposit addresses and the OKX account, the mixed use of some addresses as both initial victim deposit addresses and intermediate addresses for additional laundering, and the use of addresses to consolidate funds from multiple different victims, all of which are indicative of concealment money laundering.

**OKX ACCOUNT USER ID 373018233093155878**

111. Law enforcement back traced funds from OKX account 373018233093155878 ("5878") and identified 34 intermediary addresses between the Initial Deposit Addresses and 5878's deposit address. Law enforcement located 10 cryptocurrency confidence scam IC3 reports that reference seven of these 34 intermediary addresses. The IC3 reports describe these addresses as being linked to approximately $3,226,518.99 in victim losses to cryptocurrency confidence schemes.

112. In addition to identifiable losses, the seven addresses located in IC3 reports cumulatively received over $368 million dollars. Typically, addresses used to initially receive criminal proceeds in cryptocurrency confidence scams are likely to be utilized solely for the purpose of receiving such funds or meant to be involved in the laundering of such funds to help further obfuscate the source, control, ownership, and destination of funds.

113. This pattern of activity is illustrated in Exhibit 4 showing a series of transactions, with varying number of hops, for no apparent legitimate purpose between initial victim deposit addresses and 5878, the mixed use of some addresses as both initial victim deposit addresses and intermediate addresses for additional laundering, and use of addresses to consolidate funds from multiple different victims, all of which are indicative of concealment money laundering.

**OKX ACCOUNT USER ID 373019855340878937**

114. Law enforcement back traced funds from OKX account 373019855340878937 ("8937") and identified 40 intermediary addresses between the Initial Deposit Addresses and 8937's deposit address. Law enforcement located five cryptocurrency confidence scam IC3 reports that reference three of the 40 intermediary addresses. The IC3 reports link these four addresses to approximately $3,226,796.51 in victim losses.

115. The three addresses listed in the IC3 reports have cumulatively received over $114 million dollars in total in cryptocurrency. Typically, addresses used to initially receive criminal proceeds in cryptocurrency confidence scams are likely to be utilized solely for the purpose of receiving such funds or meant to be involved in the laundering of such funds to help further obfuscate the source and destination of funds.

116. This pattern of activity is illustrated in Exhibit 5, showing the numerous hops for no legitimate purpose, the multipurpose role of addresses being used for victim deposits and intermediate

address laundering, and the distribution and consolidation of funds traced back to reported scam addresses.

**OKX ACCOUNT USER ID 389766564775375505**

117. Law enforcement back traced funds from OKX account 389766564775375505 ("5505") and identified 48 intermediary addresses between the Initial Deposit Addresses and 5505's deposit address. Law enforcement located 21 cryptocurrency confidence scam IC3 reports that reference 10 of the 48 intermediary addresses and the victim reports link these 10 addresses to approximately $8,633,224.42 in victim losses.

118. These 10 addresses mentioned in IC3 reports have cumulatively received nearly $37 million dollars in total in cryptocurrency. Typically, addresses used to initially receive criminal proceeds in cryptocurrency confidence scams are likely to be utilized solely for the purpose of receiving such funds or meant to be involved in the laundering of such funds to help further obfuscate the source, control, ownership, and destination of funds.

119. This pattern of activity is illustrated in Exhibit 6, showing the convoluted web of transactions serving no apparent legitimate purpose, and funds flowing from and through reported scam addresses.

**OKX ACCOUNT USER ID 384292188047193948**

120. Law enforcement back-traced funds from OKX account 384292188047193948 ("3948") and identified nine intermediary addresses between the Initial Deposit Addresses and 3948's deposit address. Law enforcement identified an address that sent over $340,000 in USDT directly to one of the nine intermediary addresses. Law enforcement located one cryptocurrency confidence scam IC3 report that references this address with a reported loss of approximately $832,193.00.

121. The address listed in the IC3 report, which sends funds to one of the nine intermediary addresses, has received over $197 million dollars. Typically, addresses used to initially receive criminal proceeds of confidence scams are likely to be utilized solely for the purpose of receiving such funds or meant to be involved in the laundering of such funds to help further obfuscate the source, control, ownership, and destination of funds.

122. This pattern of activity is illustrated in Exhibit 7.

**OKX ACCOUNT USER ID 373020133213522927**

123. Law enforcement back-traced funds from OKX account 373020133213522927 ("2927") and identified 51 intermediary addresses between the Initial Deposit Addresses and 2927's deposit address. Law enforcement located nine cryptocurrency confidence scam IC3 victim reports that reference six of the 51 intermediary addresses as being linked to approximately $3,923,508.21 in victim losses.

124. These six addresses referenced in cryptocurrency confidence scam IC3 reports have cumulatively received nearly $445 million dollars in cryptocurrency. Typically, addresses used to initially receive criminal proceeds of confidence scams are likely to be utilized solely for the purpose of receiving such funds or meant to be involved in the laundering of such funds to help further obfuscate the source, control, ownership, and destination of funds.

125. This pattern of activity is illustrated in Exhibit 8, showing the convoluted web of transactions serving no apparent legitimate purpose, and funds flowing from and through reported scam addresses.

**OKX ACCOUNT USER ID 390147158499794973**

126. Law enforcement back-traced funds from OKX account 390147158499794973 ("4973") and identified 14 intermediary addresses between the Initial Deposit Address and 4973's deposit address.

Law enforcement identified 31 cryptocurrency confidence scam IC3 reports that reference one of the 14 addresses, linking this address to approximately $4,463,242.67 in victim losses.

127. The address listed in the IC3 reports has received nearly $3.3 million dollars. Typically, addresses used to initially receive criminal proceeds in cryptocurrency confidence scams are likely to be utilized solely for the purpose of receiving such funds or meant to be involved in the laundering of such funds to help further obfuscate the source, control, ownership, and destination of funds.

128. This pattern of activity is illustrated in Exhibit 9, showing the series of unnecessary hops, and even circular flow of transactions, connected to the OKX account ending in 4973.

**OKX ACCOUNT USER ID 383950945169627569**

129. Law enforcement back-traced funds from an OKX account 383950945169627569 ("7569") and identified eight intermediary addresses between the Initial Deposit Addresses and 7569's deposit address. Law enforcement identified four cryptocurrency confidence scam IC3 reports that reference one of the eight addresses as being linked to approximately $417,357.16 in victim losses to cryptocurrency confidence schemes.

130. The address listed in IC3 reports has received nearly $55,000. Typically, addresses used to initially receive criminal proceeds in cryptocurrency confidence scams are likely to be utilized solely for the purpose of receiving such funds or meant to be involved in the laundering of such funds to help further obfuscate the source, control, ownership, and destination of funds.

131. This pattern of activity, is illustrated in Exhibit 10.

**OKX ACCOUNT USER ID 386106564001588904**

132. Law enforcement back-traced funds from OKX account 386106564001588904 and identified 19 intermediary addresses between the Initial Deposit Addresses and the OKX account's deposit address. Law enforcement located two cryptocurrency confidence scam IC3 reports and an FTC

report that reference two of the 19 addresses as being linked to approximately $170,390.00 in victim losses.

133. The addresses mentioned in the IC3 and FTC reports have received over $165 million dollars in cryptocurrency in total. Typically, addresses used to initially receive criminal proceeds in cryptocurrency confidence scams are likely to be utilized solely for the purpose of receiving such funds or meant to be involved in the laundering of such funds to help further obfuscate the source, control, ownership, and destination of funds.

134. This pattern of activity is illustrated in Exhibit 11, showing the series of transactions with no identifiable legitimate purpose.

**OKX ACCOUNT USER ID 384294632080738123**

135. Law enforcement back-traced funds from OKX account 384294632080738123 ("8123") and identified 19 intermediary addresses between the Initial Deposit Address and 8123's deposit address. Law enforcement located two cryptocurrency confidence scam IC3 reports that reference two of the 19 addresses as being linked to approximately $163,086.99 in victim losses.

136. The addresses identified in IC3 reports have received nearly $11 million dollars in total. Typically, addresses used to initially receive criminal proceeds in cryptocurrency confidence scams are likely to be utilized solely for the purpose of receiving such funds or meant to be involved in the laundering of such funds to help further obfuscate the source, control, ownership, and destination of funds.

137. This pattern of activity is illustrated in Exhibit 12, showing numerous intermediary addresses sending a series of transactions over a short period of time that appear to just serve laundering purposes.

**OKX ACCOUNT USER ID 382867630484239151**

138. Law enforcement back-traced funds from OKX account 382867630484239151 ("9151") and identified 29 intermediary addresses between the Initial Deposit Addresses and 9151's deposit address. Law enforcement located one cryptocurrency confidence scam IC3 report that references one of the 29 addresses as being linked to approximately $178,141.54 in victim losses.

139. The address located on the IC3 report has received over $3 million dollars in cryptocurrency in total. Typically, addresses used to initially receive criminal proceeds in cryptocurrency scams are likely to be utilized solely for the purpose of receiving such funds or meant to be involved in the laundering of such funds to help further obfuscate the source, control, ownership, and destination of funds.

140. This pattern of activity is illustrated in Exhibit 13, showing the significant number of transactions between the reported scam address and the OKX account, among other suspicious transaction behavior.

**OKX ACCOUNT USER ID 482530396479873392**

141. Law enforcement back-traced funds from OKX account 482530396479873392 ("3392") and identified 35 intermediary addresses between the Initial Deposit Addresses and 3392's deposit address. Law enforcement located nine cryptocurrency confidence scam IC3 reports that reference seven of the 35 addresses as being linked to approximately $3,599,499.14 in victim losses.

142. The addresses located in IC3 reports have received over $12 million dollars in cryptocurrency in total. Typically, addresses used to initially receive criminal proceeds in cryptocurrency confidence scams are likely to be utilized solely for the purpose of receiving such funds or meant to be involved in the laundering of such funds to help further obfuscate the source, control, ownership, and destination of funds.

143. This pattern of activity is illustrated in Exhibit 14, showing the series of laundering transactions involving the reported scam addresses and various intermediary addresses used for further concealment of illicit funds.

**OKX ACCOUNT USER ID 382898616072852403**

144. Law enforcement back-traced funds from OKX account 382898616072852403 ("2403") and identified 65 intermediary addresses between the Initial Deposit Addresses and the OKX account's deposit address. Law enforcement located five cryptocurrency confidence scam IC3 reports that references four of the 65 intermediary addresses as being liked to approximately $3,446,890.29 in victim losses.

145. The addresses located in IC3 reports have received over $11 million dollars in cryptocurrency in total. Typically, addresses used to initially receive criminal proceeds in cryptocurrency confidence scams are likely to be utilized solely for the purpose of receiving such funds or meant to be involved in the laundering of such funds to help further obfuscate the source, control, ownership, and destination of funds.

146. This pattern of activity is illustrated in Exhibit 15, showing the significant distribution and consolidation of funds in the laundering process involving this OKX account.

**OKX ACCOUNT USER ID 373015529134418962**

147. Law enforcement back-traced funds from OKX account 373015529134418962 ("8962") and identified 30 intermediary addresses between the Initial Deposit Address and 8962's deposit address. Law enforcement located one cryptocurrency confidence scam IC3 report that referenced one of the 30 addresses as being linked to approximately $2,300,000.00 in victim losses.

148. The address listed in the IC3 report has received over $114 million dollars in total. Typically, addresses used to initially receive criminal proceeds in cryptocurrency confidence scams are likely to be utilized solely for the purpose of receiving such funds or meant to be involved in the laundering of such funds to help further obfuscate the source and destination of funds.

149. This pattern of activity is illustrated in Exhibit 16.

**OKX ACCOUNT USER ID 384001262326313296**

150. Law enforcement back traced funds from OKX account 384001262326313296 ("3296") and identified 26 intermediary addresses between the Initial Deposit Addresses and 3296's deposit address. Law enforcement located 16 cryptocurrency confidence scam IC3 reports that reference seven of the 26 addresses as being linked to approximately $2,458,610.49 in victim losses.

151. The addresses located on IC3 reports have received over $463 million dollars in total. Typically, addresses used to receive criminal proceeds are likely to be utilized solely for the purpose of receiving such funds or meant to be involved in the laundering of such funds to help further obfuscate the source and destination of funds.

152. This pattern of activity is illustrated in Exhibit 17.

**OKX ACCOUNT USER ID 436380439096268783**

153. Law enforcement back traced funds from OKX account 436380439096268783 ("8783") and identified 97 intermediary addresses between the Initial Deposit Addresses and 8783's deposit address. Law enforcement located 19 cryptocurrency confidence scam IC3 reports that reference nine of the 97 addresses as being linked to approximately $7,155,278.13 in victim losses.

154. The addresses located on IC3 reports have received over $241 million dollars in total. Typically, addresses used to initially receive criminal proceeds in cryptocurrency confidence scams are

likely to be utilized solely for the purpose of receiving such funds or meant to be involved in the laundering of such funds to help further obfuscate the source, control, ownership, and destination of funds.

155. This pattern of activity is illustrated in Exhibit 18.

**OKX ACCOUNT USER ID 389726439408283934**

156. Law enforcement back-traced funds from OKX account 389726439408283934 ("3934") and identified 21 intermediary addresses between the Initial Deposit Addresses and 3934's deposit address. Law enforcement located four cryptocurrency confidence scam IC3 reports that reference three of the 21 addresses as being linked to approximately $3,704,149.02 in victim losses.

157. The addresses referenced in IC3 reports have received over $122 million dollars in cryptocurrency in total. Typically, addresses used to initially receive criminal proceeds in cryptocurrency confidence scams are likely to be utilized solely for the purpose of receiving such funds or meant to be involved in the laundering of such funds to help further obfuscate the source, control, ownership, and destination of funds.

158. This pattern of activity is illustrated in Exhibit 19, showing the numerous transactions serving no apparent legitimate purpose involving multiple reported scam addresses and numerous intermediary addresses laundering funds.

**OKX ACCOUNT USER ID 382863414143418999**

159. Law enforcement back-traced funds from OKX account 382863414143418999 ("8999") and identified 42 intermediary addresses between the Initial Deposit Addresses and 8999's deposit address. Law enforcement located nine cryptocurrency confidence scam IC3 reports that reference four of the 42 addresses as being linked to approximately $4,906,397.86 in victim losses.

160. The addresses identified in IC3 reports have received over $37 million dollars in cryptocurrency in total. Typically, addresses used to initially receive criminal proceeds in cryptocurrency confidence cases are likely to be utilized solely for the purpose of receiving such funds or meant to be involved in the laundering of such funds to help further obfuscate the source, control, ownership, and destination of funds.

161. This pattern of activity is illustrated in Exhibit 20, showing a large series of transactions with no apparent legitimate purpose.

**OKX ACCOUNT USER ID 383132133998381393**

162. Law enforcement back-traced funds from OKX account 383132133998381393 ("1393") and identified 10 intermediary addresses between the Initial Deposit Address and 1393's deposit address. Law enforcement identified a cryptocurrency confidence scam IC3 report that referenced one of the 10 addresses as being linked to approximately $71,700.00 in victim losses.

163. The address located on the IC3 report has received over $294,000 dollars in cryptocurrency in total. Typically, addresses used to initially receive criminal proceeds in cryptocurrency confidence scams are likely to be utilized solely for the purpose of receiving such funds or meant to be involved in the laundering of such funds to help further obfuscate the source, control, ownership and destination of funds.

164. This pattern of activity is illustrated in Exhibit 21.

**OKX ACCOUNT USER ID 373874806833197907**

165. Law enforcement back-traced funds from an OKX account 373874806833197907 ("7907") and identified 29 intermediary addresses between the Initial Deposit Addresses and 7907's deposit address. Law enforcement located two cryptocurrency confidence scam IC3 reports that referenced two of the 29 addresses as being linked to approximately $500.77 in victim losses.

166. The addresses listed in the IC3 report has received over $111 million dollars in cryptocurrency in total. Typically, addresses used to initially receive criminal proceeds in cryptocurrency confidence scams are likely to be utilized solely for the purpose of receiving such funds or meant to be involved in the laundering of such funds to help further obfuscate the source, control, and ownership and destination of funds.

167. This pattern of activity is illustrated in Exhibit 22, showing numerous laundering transactions across intermediary and victim deposit addresses consolidating and further distributing funds.

**Call Center Raid and USDT Freeze**

168. During the initial investigation into ITECHNO Specialist Inc. and the cryptocurrency confidence schemes associated with the aforementioned OKX accounts, law enforcement noted a pattern of activity where funds were thoroughly laundered through exchanges, such as OKX (as detailed above), before being withdrawn and then left unspent or idle at un-hosted virtual currency addresses.

169. Many of these addresses were being monitored by law enforcement throughout the investigation. In approximately November 2023, law enforcement was advised of a planned Philippine law enforcement operation in the Manila area involving a call center containing ITECHNO Specialist Inc. This law enforcement operation at ITECHNO Specialist Inc. was reportedly halted on-site before law enforcement entered the call center.

170. Though the law enforcement operation did not occur, it appears to have triggered a substantial movement of illicit funds from some of the **SUBJECT VIRTUAL CURRENCY ADDRESSES** (which had previously been idle). Likely, the threat of a law enforcement action triggered the owners of these accounts to move funds in an effort to disguise and conceal the location, control, and

ownership of the funds and this indicated that those controlling the addresses were concerned about law enforcement intervention.

171. Specifically, USDT Token Group A (one of the **SUBJECT VIRTUAL CURRENCY ADDRESSES**), received dozens of deposits for over $155 million dollars' worth of USDT beginning on or about December 1, 2022, without a single outgoing transaction until November 15, 2023, around the time of the planned raid.

172. On or around November 20, 2023, USSS requested that Tether voluntarily freeze approximately 225 million USDT at the **SUBJECT VIRTUAL CURRENCY ADDRESSES** as part of this investigation.

## ANALYSIS OF INTERMEDIARY ADDRESSES CONSOLIDATING VICTIM FUNDS

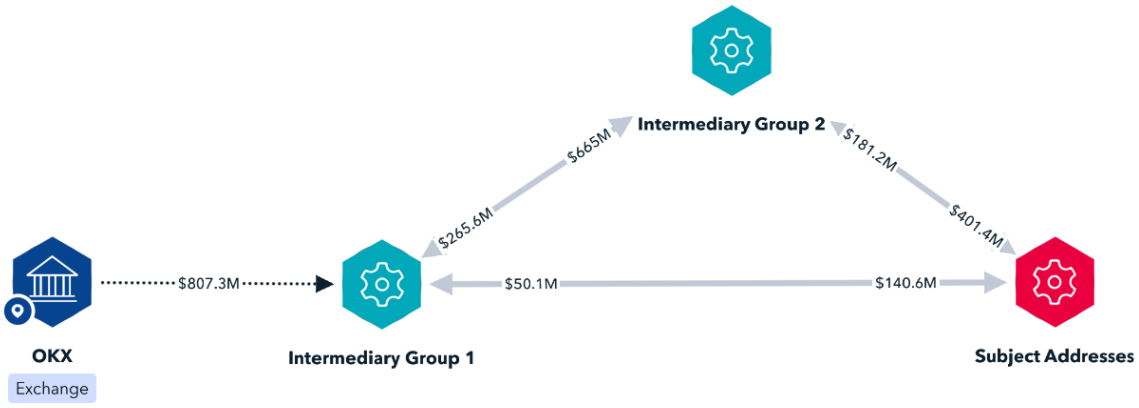
173. Law enforcement's tracing of crime proceeds in this case identified the presence of intermediary addresses that were used to consolidate funds withdrawn from OKX, including the 22 OKX Accounts. Law enforcement grouped the intermediary addresses into two groups, Intermediary Group 1 and Intermediary Group 2 ("the Intermediary Groups").

174. Intermediary Group 1 consists of 53 addresses that directly received over $800 million in virtual currency from the 144 OKX Accounts, including approximately $120 million from just the 22 OKX Accounts. Intermediary Group 1 sent approximately $665 million in virtual currency to Intermediary Group 2. Intermediary Group 1 also sent approximately $140 million in virtual currency directly to the **SUBJECT VIRTUAL CURRENCY ADDRESSES**, including approximately $44 million to USDT Token Group A, approximately $41 million to USDT Token Group B, and approximately $50 million to USDT Token Group G.

175. Intermediary Group 2 consists of 12 addresses that helped consolidate funds from Intermediary Group 1, and then transferred funds directly to the **SUBJECT VIRTUAL CURRENCY**

**ADDRESSES**, including virtual currency worth approximately $91 million to USDT Token Group A, approximately $30 million to USDT Token Group B, approximately $103 million to USDT Token Group C, approximately $3 million to USDT Token Group D, approximately $109 million to USDT Token Group E, approximately $65 million to USDT Token Group F, and approximately $20,000 to Token Group G. Token Group G also sent approximately $5.44 million to Intermediary Group 2.

176. The Intermediary Groups, along with the **SUBJECT VIRTUAL CURRENCY ADDRESSES**, also transferred hundreds of millions of dollars in virtual currency back and forth between each other in a manner that appears consistent with the repeated efforts to conceal the nature, location, source, ownership, and control of crime proceeds, and frustrate law enforcement's tracing efforts. This activity is illustrated below:




177. Among the addresses in Intermediary Group 2 are two addresses, 0xf60444fe54ff46ae29053a67e6b0fdd17b15a6b9 ("a6b9") and 0x0c0996d0c3af2892a7a8fc621eb7347ec9b6b9ac ("b9ac"). These two addresses received over $1.1 billion in funds over their lifetime. Notably, both of these addresses have served as a primary consolidation point for approximately $655,166[35] worth of funds directly traceable to confirmed and

[35] This figure accounts for tracing described in this section, as well as other tracing for two additional OKX accounts with addresses ending in "ed53" and "fa5d," referenced within paragraph 207 below.

likely victims of cryptocurrency confidence scams, including G.B., as detailed below. The consolidation addresses ending in a6b9 and b9ac sent approximately $62.4 million and $197.2 million in virtual currency, respectively, to the **SUBJECT VIRTUAL CURRENCY ADDRESSES**.

**OKX UID: 382863414143418999**

178. Between on or about March 18, 2023, and on or about March 19, 2023, OKX UID 382863414143418999 (one of the 144 OKX accounts) received deposits totaling approximately 361,000 USDT into the deposit address 0x7f2de657ab21f269ea8e37eea1a9245af6d2e669. During the same period, the OKX account conducted an equal number of withdrawals within minutes of the deposits, all to address 0x517adbbe7ebd0a2096f11fbaa5ed2988844a8d73. Using LIFO, those funds ultimately were traced into the a6b9 consolidation address.

179. Back-tracing of the original 361,000 USDT deposits identified six individuals believed to be victims of cryptocurrency confidence scams, including four that have confirmed to law enforcement that their transactions are the result of such scams. These six individuals sent cryptocurrency worth approximately $632,332.67 to initial deposit addresses identified in the back-tracing, a portion of which includes seven deposits totaling over $270,000 worth of virtual currency. Following LIFO, approximately $263,000[36] in virtual currency can be traced to the a6b9 consolidation address. This flow of funds, which included the use of 42 intermediary addresses prior to depositing into OKX, is illustrated below:


[36] During the laundering process, some hops left behind portions of funds, or transferred them to other addresses, reducing the LIFO traced amount from the original deposited amount.

**OKX UID: 382867630484239151**

180. On or about January 4, 2023, OKX UID 382867630484239151 (one of the 144 OKX accounts) received deposits totaling nearly 123,000 USDT into deposit address 0x3d60b144585958fcf0887ec7f3e0fa9eaeacb82a. On the same day, the OKX account conducted an equal number of withdrawals within minutes of the deposits, all to address 0x517adbbe7ebd0a2096f11fbaa5ed2988844a8d73. Using LIFO, those funds ultimately were deposited to the a6b9 consolidation address, through the b9ac consolidation address.

181. Back-tracing of the original 123,000 USDT deposits identified 25 individuals believed to be victims of cryptocurrency confidence scams, including two that have confirmed to law enforcement that their transactions are the result of such scams. These 25 individuals sent approximately $217,182.46 to initial deposit addresses identified in the back-tracing, a portion of which includes four deposits totaling 28,000 USDT. Following LIFO, all 28,000 USDT can be traced to the a6b9 consolidation address. This flow of funds, which included the use of 29 intermediary addresses prior to depositing into OKX, is illustrated in Exhibit 23:

**OKX UID: 382898616072852403**

182. Between on or about December 27, 2022, and on or about January 4, 2023, OKX UID 382898616072852403 (one of the 144 OKX accounts) received deposits totaling nearly 3.57 million USDT into deposit address 0x6f7b333af41dffe89c10820243327a71d1926b0f. During the same period, the OKX account conducted a nearly equal number of withdrawals within minutes of the deposits, all to address 0x732afda0d3e88611a2b2c8ffb0428486619f35a5. Following LIFO, those funds ultimately were deposited to the a6b9 consolidation address, through the b9ac consolidation address.

183. Back-tracing of the original 3.57 million USDT deposits identified 19 individuals believed to be victims of cryptocurrency confidence scams, including eight that have confirmed to law

enforcement that their transactions were the result of such scams. These 19 individuals sent approximately $754,957.86 in virtual currency to initial deposit addresses identified in the back-tracing, a portion of which includes 24 deposits totaling over $287,000 USDT. Following LIFO, approximately $250,000 worth of virtual currency can be traced to the a6b9 consolidation address. This flow of funds, which included the use of 64 intermediary addresses prior to depositing into OKX, is illustrated in Exhibit 24.

**OKX UID: 389726439408283934**

184. On or about May 21, 2023, OKX UID 389726439408283934 (one of the 144 OKX accounts) received deposits totaling over 106,000 USDT into deposit address 0xb7306f55e4832b3e687784784cd163519084c0dc. On the same day, the OKX account conducted an equal number of withdrawals within minutes of the deposits, all to address 0xe8b4b6bee0f6b913b847a7b850cc02bbde30d506. Using LIFO, those funds ultimately were deposited to the b9ac consolidation address.

185. Back-tracing of the original 106,000 USDT deposits identified 10 individuals believed to be victims of cryptocurrency confidence scams, including two that have confirmed to law enforcement that their transactions are the result of such scams. These 10 individuals sent approximately $377,184.30 to initial deposit addresses identified in the back-tracing, a portion of which includes eight deposits totaling nearly 78,000 USDT. Following LIFO, approximately $7,700 in virtual currency can be traced to the b9ac consolidation address. This flow of funds, which included the use of 21 intermediary addresses prior to depositing into OKX, is illustrated in Exhibit 25:

**OKX UID: 436380439096268783**

186. Between on or about May 13, 2023, and May 14, 2023, OKX UID 436380439096268783 (one of the 144 OKX accounts) received deposits totaling over 131,000 USDT into deposit address 0x029b12327a9b5b1964d3da841a376c9934d5bbf4. During the same time period, the OKX account conducted a nearly equal number of withdrawals within minutes of the deposits, all to address 0x150f39c4fc18e05a138dd5d56e35400643bd7cc7. Using LIFO, those funds ultimately were deposited to the 5a6b9 consolidation address, through the b9ac consolidation address.

187. Back-tracing of the original 131,000 USDT deposits identified eight individuals believed to be victims of cryptocurrency confidence scams, including one that has confirmed to law enforcement that their transactions are the result of such a scam. These eight individuals sent approximately $86,195.23 to initial deposit addresses identified in the back-tracing, a portion of which includes one deposit totaling over 71,000 USDT. Following LIFO, approximately $40,000 in virtual currency can be traced to the a6b9 consolidation address. This flow of funds, which included the use of 11 intermediary addresses prior to depositing into OKX, is illustrated in Exhibit 26:

## GAS FEE ANALYSIS & CONNECTIONS, INCLUDING TO SUBJECT VIRTUAL CURRENCY ADDRESSES

188. Law enforcement analyzed the source of network gas fees received into the Intermediary Group 2 addresses and the **SUBJECT VIRTUAL CURRENCY ADDRESSES** and determined that they presented strong connections to the 144 OKX Accounts. Blockchain networks, such as the Ethereum network, where the funds relevant to this affidavit were transacted on, require fees to be paid in that network's native virtual currency. In the case of Ethereum, that native asset is ETH. Though this affidavit primarily discusses the laundering of USDT, the movement of the USDT was facilitated through gas fees

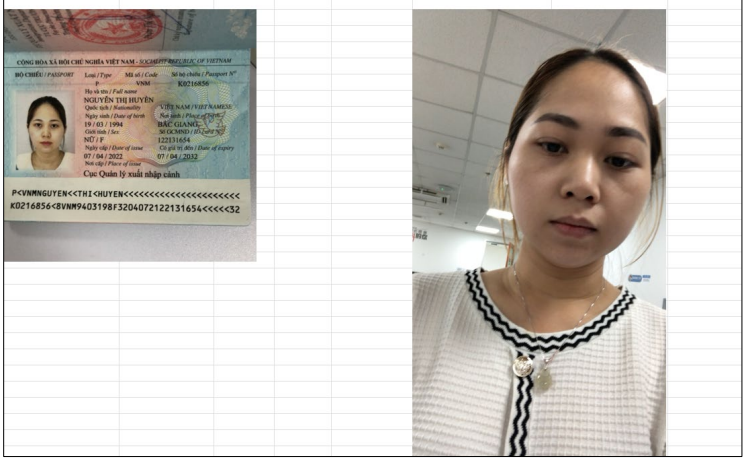
paid in ETH. The following analysis details the gas payments and their connections between the OKX accounts and the Intermediary Group 2 addresses.

189. As illustrated in Exhibit 27, the two primary consolidation addresses, a6b9 and b9ac, provided the ETH funding, in some cases directly, to the remaining 10 intermediary addresses:[37]

190. Law enforcement further back-traced the source of ETH from the 5a6b9 and b9ac consolidation addresses to three OKX accounts, OKX UID 316574636496327938, OKX UID 430669787564277712, and OKX UID 316573777658046610. OKX UID 316573777658046610 and OKX UID 430669787564277712 were already identified as being part of the 144 OKX Accounts, while OKX UID 316574636496327938 has account subscriber characteristics that appear to link the account to the same scheme. For example, the three OKX accounts maintain the same or similar email naming convention (i.e., 'c' or letters followed by ten numbers (corresponding with their mobile numbers), @icloud.com), are registered to Vietnamese owners, and at least two of the accounts appear to have KYC photos potentially taken within the same office. OKX UID 316573777658046610 and OKX UID 316574636496327938 were also created within three minutes of each other, as seen below:

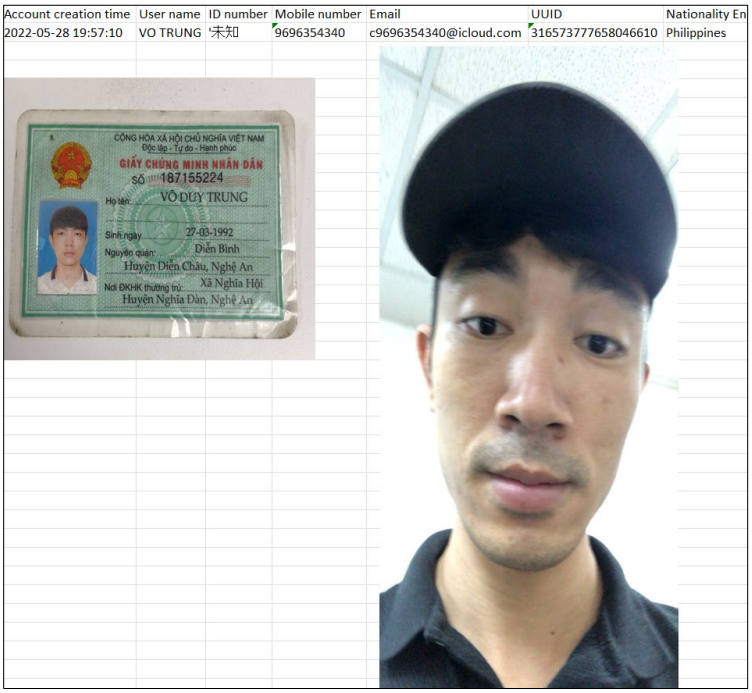
OKX UID 316574636496327938

| Account creation time | User name | Nationality | ID number | Mobile number | Email | UUID | Nationality En |
|---|---|---|---|---|---|---|---|
| 2022-05-28 20:00:35 | Nguyen Thi Huyen | 越南 | K0216856 | 9695613047 | c9695613047@icloud.com | 316574636496327938 | Vietnam |




[37] Intermediary Group 2 addresses are notated in Orange.

OKX UID 316573777658046610




OKX UID 430669787564277712


191. The following analysis details the gas fee payments and their connections between some of the 144 OKX Accounts and most of the **SUBJECT VIRTUAL CURRENCY ADDRESSES**. The results of this analysis indicate that those who control multiple **SUBJECT VIRTUAL CURRENCY ADDRESSES** also control at least some of these OKX accounts which were also used for laundering purposes.

**USDT Token Group B, E, and F**

192. As illustrated in Exhibit 28, the gas payment for USDT Token Group B, E, and F, which originates from the b9ac address from Intermediary Group 2, can be traced back to OKX UID 316574636496327938 and OKX UID 430669787564277712. Although the OKX UID 316574636496327938 account is not one of the 144 OKX Accounts, this account is also consistent with the same characteristics previously mentioned, such as being registered to a Vietnamese national in the Philippines and uses the consistent email naming convention. Additionally, this account is accessed by at least one IP address that has also accessed two of the 144 OKX Accounts. Specifically, IP 175.176.40.38 was used to access this user's account, as well as that of OKX UID 405579019917082264 and 373874806833197907.

**USDT Token Group C**

193. As illustrated in Exhibit 29, the gas payment for USDT Token Group C originates from the a6b9 address from Intermediary Group 2, which can be traced back to OKX Account with UID 316573777658046610. This account's registration information is consistent with the same characteristics previously mentioned, such as being registered to a Vietnamese national in the Philippines and using the consistent email naming convention. The same email address was also used for another OKX account, UID 428375340373973826, which is one of the 144 OKX Accounts.

**USDT Token Group G**

194. As illustrated in Exhibit 30, the gas payment for USDT Token Group G originates from OKX Account with UID 299286355324882944. This account is also consistent with the same characteristics previously mentioned, such as being registered to a Vietnamese national in the Philippines and using an iCloud email account.

195. Cumulatively, these five USDT Token Groups with gas fee connections to these three OKX accounts represent over 85% of the combined balance of funds sought in this complaint. This likely demonstrates that the owners of the USDT Token Groups are also the owners of the three OKX accounts. This further solidifies the connection of the 144 OKX accounts to the **SUBJECT VIRTUAL CURRENCY ADDRESSES**. It shows that the owners of the three OKX accounts discussed in this section, two of which were involved in receiving fraud proceeds and engaging in money laundering, paid transactions fees to move laundered fraud funds from the 144 OKX Accounts into the **SUBJECT VIRTUAL CURRENCY ADDRESSES,** where the funds currently sit.

## LAUNDERING AND TRACING EXAMPLE FROM AN INITIAL VICTIM DEPOSIT ADDRESS TO A SUBJECT VIRTUAL CURRENCY ADDRESS

196. The launderers' use of sophisticated money laundering techniques presents numerous complex challenges to investigators when tracing victim funds from their initial deposit addresses all the way to the **SUBJECT VIRTUAL CURRENCY ADDRESSES**. These challenges include the sheer volume of transactions involved in the network of 144 OKX Accounts (hundreds of thousands), the use of consolidation addresses used to accumulate hundreds of millions of dollars that redirects the LIFO order, and the use of countless intermediary addresses that serve to both add additional difficulty to the tracing efforts and also redirect the LIFO order. Nevertheless, using LIFO, investigators were able to trace some victim funds in initial deposit addresses to some of the **SUBJECT VIRTUAL CURRENCY ADDRESSES**. One such example is illustrated in Exhibit 31. Exhibit 31 condenses transactions in arrows (describing multiple transactions) and shapes described as intermediary addresses to streamline the illustration of the flow of funds.

197. The chart above illustrates the following flow of funds undertaken to launder victim funds, namely:

198. Law enforcement interviewed Victim G.B., who confirmed that she was the victim of a cryptocurrency confidence scam. G.B. sent approximately 37,566 USDT to an initial deposit address, which then sent the entirety of G.B.'s funds within a few minutes to a consolidation address, and then along to a series of additional addresses, all labeled as "13 Intermediary Addresses" above.

199. Victim G.B.'s funds were traced to the address ending in "f5f8" in the chart above. f5f8 then engaged in multiple circular transactions with several addresses, which serve no apparent legitimate business or financial purpose and were likely undertaken for laundering purposes.

200. f5f8 sent some of Victim G.B.'s funds to the address ending in "b5ec" as part of an withdrawal worth approximately 1,329,000 USDT. b5ec was likely used as a consolidation address to commingle funds from other suspected victims who sent funds from Coinbase and Kraken accounts.[38]

201. b5ec then distributed funds, including some of Victim G.B.'s, in three nearly equal amounts of approximately 500,000, 500,000, and 499,980 USDT to three addresses, all within a day. While one of the receiving addresses sent the funds it received into an address that funded circular transactions with f5f8, the other two addresses (ending in "45d8" and "8c7d") sent the 500,000 USDT they both received to addresses ending in "4547" and "cf24," respectively, both within an hour of receiving the 500,000 USDT. There is no logical economic purpose for transacting this way and are clearly for laundering purposes.

202. Then, "4547" and "cf24" each sent 21 transfers, respectively, to separate OKX accounts, ending in "ed53" and "fa5d." These two OKX accounts are among the 22 OKX Accounts described above. The subjects' use of these OKX accounts was likely to help break the publicly visible flow of funds on the blockchain, requiring law enforcement to have to seek records from the exchange to

[38] The transaction history from the Coinbase and Kraken accounts listed on the chart above are consistent with transaction histories for confirmed victims who sent funds into the 144 OKX Accounts money laundering network. These victims are likely in the United Kingdom.

determine the connection between deposits and withdrawals. In other words, the use of OKX accounts and infrastructure served the purpose of concealing or disguising the location, source, ownership, or control of funds, including Victim G.B.'s funds.

203. As with other tracing examples described above, the subjects then moved funds from the OKX accounts in a large number of transfers (42) to multiple additional addresses (seven). The deposits into the OKX accounts had corresponding 1:1 withdrawals, further evidencing that the OKX accounts were used for concealment laundering purposes. One of these addresses, ending in "b9ac," then deposited approximately 4,529,900 USDT into **USDT Token Group E**, which includes approximately 4,466 USDT of funds traceable to Victim G.B.

204. The b9ac address that sent the transaction to **USDT Token Group E** containing Victim G.B.'s funds also sent approximately 15,890,000 USDT to another address ending in "2c91," which then sent funds back to b9ac through a third address, 80ec, all within the span of two months.[39] This type of movement is common among cryptocurrency launderers to avoid leaving large USDT balances in single addresses for too long, leaving them susceptible to potential freezes. These circular transactions, coupled with the large volume of transfers described in the paragraph above, are additional evidence of the laundering use of the addresses to transfer, conceal, and obfuscate victims' funds.

## The SUBJECT VIRTUAL CURRENCY ADDRESSES

205. For each of the **SUBJECT VIRTUAL CURRENCY ADDRESSES**, law enforcement traced the flow of funds (as described above) from the 22 OKX Accounts through additional OKX accounts, to include the other 122 OKX accounts controlled by this group, to one or more of the **SUBJECT VIRTUAL CURRENCY ADDRESSES** where funds were frozen.

[39] These transactions are not shown in Exhibit 31.

206. The blockchain tracing revealed apparent money laundering activity. For example, the ways in which the criminal actors withdrew funds from the 144 OKX Accounts was indicative, of efforts to obscure the source of the funds. Those efforts included the use of 35 intermediary addresses (the "35 intermediary addresses") between some of the 144 OKX Accounts and the **SUBJECT VIRTUAL CURRENCY ADDRESSES** to further conceal the fact that the funds came from some of the 144 OKX Accounts.

**USDT Token Group A**

207. As illustrated in Exhibit 32,[40] USDT Token Group A received funds through 29 of the 35 suspect-controlled intermediary addresses[41] for a total of approximately 135,369,876 USDT to USDT Token Group A in a funnel-like pattern indicative of concealment money laundering. These suspect-controlled addresses appear to have been used as pass-through addresses to send victim funds from OKX to the **SUBJECT VIRTUAL CURRENCY ADDRESSES**, acting as consolidation addresses. As described above, consolidation addresses are used to commingle different victims' funds after launderers have dispersed them across many separate addresses to disguise the location, control, and ownership of the funds.

208. The analysis identified that 19 of the 35 suspect-controlled intermediary addresses referenced above received over 24,000 transfers directly from 117 of the 144 OKX Accounts for approximately 370,109,739 USDT between on or about November 15, 2022, and September 19, 2023.

[40] The red dot denotes Token Group A. The top dot denotes some of 144 OKX Accounts.

[41] These 35 intermediary wallets were identified as being launderer-controlled because they were all used to help launder funds passing from the 144 OKX Accounts to the **SUBJECT VIRTUAL CURRENCY ADDRESSES**, both of which are also believed to be controlled by the same group of cryptocurrency confidence scam money launderers.

209. USDT Token Group A maintained a balance of approximately 29,413,681 USDT before its tokens were burned and reissued pursuant to their seizure.

**USDT Token Group B**

210. Further analysis of the withdrawal activity from the 22 OKX Accounts and the 35 intermediary addresses determined that seven of the intermediary addresses were used to funnel approximately 71,464,540 USDT to USDT Token Group B.

211. The analysis identified that six of the suspect-controlled intermediary addresses referenced above received over 2,000 transfers directly from 114 of the 144 OKX Accounts for approximately 91,978,571 USDT.

212. The flow of funds through the seven suspect-controlled intermediary addresses to USDT Token Group B is illustrated in Exhibit 33.[42] Note the similar consolidation of funds before they were sent to USDT Token Group B.

213. USDT Token Group B maintained a balance of approximately 30,000,000 USDT before the tokens were burned and reissued pursuant to their seizure.

**USDT Token Group C**

214. Further withdrawal analysis from the 144 OKX Accounts and the 35 intermediary addresses between the 144 OKX Accounts and the **SUBJECT VIRTUAL CURRENCY ADDRESSES** determined that six of the 35 intermediary addresses were used to funnel approximately102,816,042 USDT to USDT Token Group C.

[42] The red dot denotes Token Group B. The top dot denotes some of 144 OKX Accounts.

215. The analysis identified that five of the suspect-controlled intermediary addresses referenced above received nearly 400 transfers directly from 26 of the 144 OKX Accounts for approximately 6,247,429 USDT.

216. The flow of funds through the six suspect-controlled intermediary addresses to USDT Token Group C is illustrated in Exhibit 34.[43] Note the consolidation of funds before they were sent to USDT Token Group C, consistent with the laundering of funds for the other token groups. USDT Token Group C maintained a balance of approximately 8,737,742 USDT before the tokens were burned and reissued pursuant to their seizure.

**USDT Token Group D**

217. Law enforcement's analysis of the activity connected to the 35 intermediary addresses determined that 17 of those addresses were used in the same funnel-like pattern to launder approximately 2,999,900 USDT from some of the 144 OKX Accounts to USDT Token Group D.

218. The analysis identified that 16 of those 35 suspect-controlled intermediary addresses received over 19,000 transfers directly from 55 of the 144 OKX Accounts for approximately 244,505,536 USDT.

219. The flow of funds through the 17 suspect-controlled intermediary addresses to USDT Token Group D is illustrated in Exhibit 35.[44] There is a significant consolidation of funds into an intermediary address before being sent to USDT Token Group D.

220. USDT Token Group D maintained a balance of approximately 2,903,914 USDT before the tokens were burned and reissued pursuant to their seizure.

**USDT Token Group E**

[43] The red dot denotes Token Group C. The top dot denotes some of 144 OKX Accounts.

[44] The red dot denotes Token Group D. The top dot denotes some of 144 OKX Accounts.

221. Law enforcement's analysis of the activity connected to the 35 suspect-controlled intermediary addresses determined that 25 of 35 intermediary addresses were used in the same funnel-like pattern to launder approximately 76,891,075 USDT from the 144 OKX Accounts to USDT Token Group E.

222. The analysis identified that 17 of those 35 suspect-controlled intermediary addresses received over 22,000 transfers directly from 57 of the 144 OKX Accounts for approximately 284,082,297 USDT.

223. The flow of funds through the 25 suspect-controlled intermediary addresses to USDT Token Group E is illustrated in Exhibit 36.[45] The disbursed set of funds were consolidated into a handful of addresses, before being consolidated into one address, which sent its funds to USDT Token Group E:

224. USDT Token Group E maintained a balance of approximately 2,137,276 USDT before the tokens were burned and reissued pursuant to their seizure.

**USDT Token Group F**

225. Additional analysis of the activity connected to the 35 suspect-controlled intermediary addresses determined that 25 of those addresses were used in the same funnel-like pattern to launder approximately 64,707,697 USDT from some of the 144 OKX Accounts to USDT Token Group F, including 17 suspect-controlled addresses that received over 22,000 transfers directly from 56 of the 144 OKX Accounts for approximately 284,082,297 USDT.

[45] The red dot denotes Token Group E. The top dot denotes some of 144 OKX Accounts.

226. The flow of funds through 25 of the 35 suspect-controlled intermediary addresses to USDT Token Group F is illustrated in Exhibit 37.[46] USDT Token Groups E and F received their funds from the same intermediary addresses.

227. USDT Token Group F maintained a balance of approximately 64,707,709 USDT before the tokens were burned and reissued pursuant to their seizure.

**USDT Token Group G**

228. Law enforcement's analysis of the activity connected to the 35 suspect-controlled intermediary addresses determined that 17 of 35 intermediary addresses were used in the same funnel-like pattern to launder approximately 59,017,221 USDT from some of the 144 OKX Accounts to USDT Token Group G, including 15 suspect-controlled addresses that received over 18,000 transfers directly from 59 of the 144 OKX Accounts for approximately 275,290,394 USDT.

229. The flow of funds through 17 of the previously identified 35 suspect-controlled intermediary addresses to USDT Token Group G is illustrated in Exhibit 38.[47] Note the use of two consolidation intermediary addresses before funds were sent to the USDT Token Group G.

230. USDT Token Group G maintained a balance of approximately 87,464,642 USDT before the tokens were burned and reissued pursuant to their seizure.

**Summary of the SUBJECT VIRTUAL CURRENCY ADDRESSES**

231. A holistic analysis of the **SUBJECT VIRTUAL CURRENCY ADDRESSES** reveals that each interacted with the 35 suspect-controlled intermediary addresses that received funds from the 144 OKX Accounts. 24 of the 35 suspect-controlled intermediary addresses, and USDT Token Group G,

[46] The red dot denotes Token Group F. The top dot denotes some of 144 OKX Accounts.

[47] The red dot denotes Token Group G. The top dot denotes some of 144 OKX Accounts.

cumulatively received approximately 435,354,370 USDT directly from some of 144 OKX Accounts.[48] The 35 intermediary addresses in between the 144 OKX Accounts and the **SUBJECT VIRTUAL CURRENCY ADDRESSES** were involved in a complex pattern of fund transfers that appear designed to conceal the nature, source, location, ownership, and control of funds. This pattern, in Exhibit 39, utilized 35 addresses to launder funds known to be connected to cryptocurrency confidence schemes through OKX. [49]

232. Additionally, 24 of the 35 suspect-controlled intermediary addresses, and USDT Token Group G, received funds directly from over 130 of the 144 OKX Accounts. In many instances, the transfers were for similar amounts. For example, over 14,000 transfers were made in amounts between approximately 9,000 USDT and 11,000 USDT. The sheer volume of transactions makes tracing each transaction extremely time and resource intensive.

233. In many instances, many of the 144 OKX Accounts were involved in the transfer activity on the very same day to the same recipient addresses in a pattern indicative of concealment money laundering.

234. For example, two of the 144 OKX Accounts featured nearly identical transfer activity to the same recipient address on the same day. Specifically, on or about September 18, 2023, one user initiated a small value transaction that appears to have been a test transaction, followed by 13 transfers to one of the 35 suspect-controlled intermediary addresses for a total of approximately 249,896 USDT. On the same day, another user also initiated an apparent test transaction, followed by 13 transfers to the same suspect-controlled intermediary address for a total of approximately 252,008 USDT.

---

[48] Many, but not all, of the 144 OKX Accounts transacted with the 35 intermediary addresses.

[49] The 144 OKX Accounts are denoted in the graph as the upper center hexagon. The 35 suspect-controlled intermediary addresses are denoted as grey dots. The **SUBJECT VIRTUAL CURRENCY ADDRESSES (A, B, C, D, E, F, and G)** are denoted by red dots.

235. Cumulatively, the **SUBJECT VIRTUAL CURRENCY ADDRESSES** received approximately 513,266,351 USDT from the 35 suspect-controlled intermediary addresses, which can be traced back to many of the 144 OKX Accounts. This high value amount and volume of transactions, moved in this fashion, is indicative of money laundering.

236. As previously noted from the FATF Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing report, one of the red flag indicators related to transaction patterns includes making frequent transfers in a certain period of time to the same virtual asset account by more than one person; from the same IP address by one or more persons; or concerning large amounts. Other red flags include the size and frequency of transactions. This includes converting the virtual assets to multiple virtual assets, incurring additional transaction fees without logical business explanations (e.g., portfolio diversification), or withdrawing the virtual assets from a virtual asset service provider ("VASP") immediately to an unhosted wallet. This effectively turns the exchange/VASP into a money laundering mixer.[50]

237. Individuals engaged in money laundering often move proceeds of criminal activity through multiple financial accounts, including virtual currency wallets, frequently at a rapid pace, and often with no discernable legitimate purpose. Such individuals move proceeds in this fashion to hide the financial connection between the illegal activity and the ultimate account. The rapid movement of funds transferred from one address to another on the same blockchain, in the manner described above, has no economic justification and is instead indicative of efforts to commit concealment money laundering by obfuscating the flow and true source of funds. This is highlighted by the presence of 35 suspect-controlled intermediary addresses and over 25,000 transfers between the 144 OKX Accounts and the **SUBJECT**

[50]The Financial Action Task Force, *FATF REPORT Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing* https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-Red-Flag-Indicators.pdf.coredownload.pdf (Sept. 2020).

**VIRTUAL CURRENCY ADDRESSES**. Each transfer incurred fees between approximately $1 and $5 at the time of the transaction, adding up to between $25,000 and $125,000 worth of fees, which would be cost-ineffective for any legitimate activity. Additionally, the transaction behavior where funds are sent to many addresses, only to subsequently consolidate into a few addresses in what would visually appear to depict two funnels with the narrow part at either end has no apparent legitimate purpose and merely exists to complicate tracing efforts. The blockchain analysis in this case demonstrates such conduct. Specifically, the movement of the victims' funds, received into an exchange, broken up, distributed through a series of virtual currency addresses, and re-consolidated with other funds into the **SUBJECT VIRTUAL CURRENCY ADDRESSES** indicates money laundering. The existence of these convoluted, intermingled, and re-consolidated transactions—which incurred transaction fees and served no apparent legitimate purpose—imply that the purpose of these numerous, fast-repeating, and intermingled transactions was to conceal the nature, source, location, ownership and control of the proceeds. As such, the **SUBJECT VIRTUAL CURRENCY ADDRESSES** facilitated and were "involved in" the commission of concealment money laundering and are thus subject to forfeiture.

238. Additionally, in light of law enforcement's determination that the 144 OKX Accounts, which received traced and suspected cryptocurrency confidence scam proceeds, were opened in the names and identities of individuals believed to be unrelated to the actual control or ownership of funds, likely in an effort to conceal the true ownership or connections to known and unknown coconspirators, the **SUBJECT VIRTUAL CURRENCY ADDRESSES** were used to commit concealment money laundering as the ultimate recipient of many of the funds transferred out of the 144 OKX accounts.

**Outreach From Potential Claimants**

239. In or around June 2024, an attorney from an international law firm claimed that their client owned the funds associated with five of the **SUBJECT VIRTUAL CURRENCY ADDRESSES**. Over

the course of six months, counsel never provided answers to simple ownership questions concerning the full legal name of the company, where their offices are located, or whether the company had a public facing website. After nearly six months of the investigative team requesting basic information, counsel informed the United States that his representation had ended.

240. In or around February 2025, an attorney from another law firm contacted the United States on behalf of a client claiming that they owned the funds associated with five of the **SUBJECT VIRTUAL CURRENCY ADDRESSES**. The attorney stated that their client was an online gaming/gambling company named Infiniweb Technology, Inc. Open-source research regarding Infiniweb revealed minimal information about the company, including an article stating that the company "is understood to have close links with Xionwei Technologies, which is accused of being involved in kidnapping and human trafficking. The accusations of kidnapping and human trafficking were outlined in a 120-page report from 2023, submitted to the nineteenth congress of the Republic of the Philippines."[51] Inifiniweb was also listed on a "LIST OF CANCELLED OFFSHORE GAMING LICENSEES," appearing to be dated January 15, 2024, posted by the Philippine Amusement and Gaming Corporation.[52] The law firm representing Infiniweb has not provided the United States with any additional information showing that the funds associated with the **SUBJECT VIRTUAL CURRENCY ADDRESSES** are derived from lawful sources, unrelated to cryptocurrency confidence scams or other criminal activity.

[51] Philippe Auclair, Andy Brown, Jack Kerr, Samindra Kunti, Steve Menary, *Meet the hydras: tracing the illegal gambling operators that sponsor football* https://www.playthegame.org/news/meet-the-hydras-tracing-the-illegal-gambling-operators-that-sponsor-football/ (Jan. 30, 2024).

[52] Philippine Amusement and Gaming Corporation, *List Of Cancelled Offshore Gaming Licensees,* https://www.pagcor.ph/regulatory/pdf/offshore/list-of-cancelled-offshore-gaming-licensees.pdf (Jan. 15, 2024).

**COUNT ONE – FORFEITURE OF DEFENDANT PROPERTY**
**(18 U.S.C. § 981(a)(1)(C))**

241. The paragraphs contained in this complaint are herein realleged and incorporated by reference.

242. The Defendant Property includes property constituting or derived from proceeds traceable to wire fraud and conspiracy to commit wire fraud, in violation of 18 U.S.C. §§ 1343 and 1349.

243. Accordingly, the Defendant Property is subject to forfeiture to the United States under 18 U.S.C. § 981(a)(1)(C).

**COUNT TWO – FORFEITURE OF DEFENDANT PROPERTY**
**(18 U.S.C. § 981(a)(1)(A))**

244. The paragraphs contained in this complaint are herein realleged and incorporated by reference.

245. The Defendant Property constitutes property involved in concealment money laundering transactions committed in violation of Title 18, United States Code, Sections 1956(a)(1)(B)(i) and conspiracy to engage in money laundering, committed in violation of Title 18, United States Code, Section 1956(h).

246. Accordingly, the Defendant Property is subject to forfeiture to the United States under 18 U.S.C. § 981(a)(1)(A).

**PRAYER FOR RELIEF**

WHEREFORE, the United States of America prays that notice issue on the Defendant Property as described above; that due notice be given to all parties to appear and show cause why the forfeiture should not be decreed; that this Honorable Court issue a warrant of arrest *in rem* according to law; that judgment be entered declaring that the Defendant Property be forfeited to the United States of America for disposition according to law; and that the United States of America be granted such other relief as this Court may deem just and proper.

June 18, 2025
Washington, D.C.

Respectfully submitted,

JEANINE FERRIS PIRRO
United States Attorney

*/s/ Rick Blaylock, Jr.*
Rick Blaylock, Jr.
TX Bar No. 24103294
Assistant United States Attorney
Asset Forfeiture Coordinator
United States Attorney's Office
601 D Street, N.W.
Washington, D.C. 20001
(202) 252-6765
rick.blaylock.jr@usdoj.gov

**VERIFICATION**

I, Meredith Williams, a Special Agent with the Federal Bureau of Investigation, declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the foregoing Verified Complaint for Forfeiture *in rem* is based upon reports and information known to me and/or furnished to me by other law enforcement representatives and that everything represented herein is true and correct.

Executed on this 18 th day of June 2025.

Meredith Williams

Meredith Williams,
Special Agent
Federal Bureau of Investigation