UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA **v.** **APPROXIMATELY 927,155.442 USDT** **Defendant, *in rem.***	§ § § § § § § § §	**COMPLAINT FOR FORFEITURE *IN REM*** ***CIVIL ACTION NO.*** **25-cv-3914**

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 927,155.442 USDT, hereinafter referred to as "Defendant Property", and alleges as follows:

STATEMENT OF THE CASE

1. Criminals believed to be located abroad, their associates, and conspirators together stole funds from at least 13 victims. The funds were then laundered through a series of virtual currency addresses, and some virtual currency exchanges, to evade detection and hide the origin of the funds. The Federal Bureau of Investigation (FBI), investigated, traced, and seized 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, and most importantly, to recover assets that may be used to compensate victims.[1]

[1] *See* United States Asset Forfeiture Program, *Our Mission*, https://www.justice.gov/afp.

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) and (b).

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(a)(2)(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 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. 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. 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. 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 of money laundering.

13. 18 U.S.C. § 1956(a)(2)(B)(i) provides that whoever transports, transmits, or transfers, or attempts to transport, transmit, or transfer a monetary instrument or funds from a place in the United States to or through a place outside the United States or to a place in the United States from or through a place outside the United States—knowing that the monetary instrument or funds involved in the transportation, transmission, or transfer represent the proceeds of some form of

unlawful activity and knowing that such transportation, transmission, or transfer 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, commits international money laundering.

14. 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.

PROPERTY INFORMATION

15. The Defendant Property is 927,155.442 USDT, which is the equivalent to $ 927,155.442 in U.S. dollars (USD). The Defendant Property is associated with virtual currency addresses:

0xD365849035325A1a49bD43F5F43063F1AEC0Ccd6 (Subject Address 1);

0x3760Cd4E92F8bAe88bC4541bf5a8A5531eeA2C80 (Subject Address 2);

0x2341E30EacD99d3cB3F9b7831144C82be18157c2 (Subject Address 3);

0xa6173A4128Bb9aDEf4fBE4D858363FbcdA23c089 (Subject Address 4); and

0x4663c4dF09D4dD347197507defD1551b6Ce10067 (Subject Address 5);

(collectively the "Subject Addresses"), which collectively held 927,155.442 USDT. The currency previously associated with the Subject Addresses is hereinafter referred to as the "Defendant Property."

16. The Defendant Property is currently in custody and control of the United States.

STATEMENT OF FACTS

Background on Cryptocurrency

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 and Ether, 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 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 (or "ETH") 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. Virtual Currency Exchange: A virtual currency exchange ("VCE"), also called a virtual currency 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).

22. 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.

23. 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. Unhosted wallets allow users to generate and manage their own unhosted wallet addresses.

24. Hosted Wallet: A hosted wallet, also known as a custodial wallet, is a virtual currency wallet through which a third party, e.g., a virtual currency exchange, holds a user's private keys. The third party maintains the hosted wallet on its platform akin to how a bank maintains a bank account for a customer, allowing the customer to authorize virtual currency transactions involving the hosted wallet only by logging into/engaging with the third party's platform.

25. 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.

26. 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 ("ETH"), 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.

27. 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.

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

29. Ether: Ether ("ETH") is a virtual currency that is the native token used by the Ethereum blockchain, which is a blockchain with smart contract functionality.

Background on Cryptocurrency Investment Fraud

30. The FBI is investigating cryptocurrency investment fraud ("CIF") schemes, often referred to as "pig-butchering," a term derived from the Chinese-language word used to describe this scheme and its treatment of victims. In 2024 alone, more than 41,000 complaints of CIF were received by the FBI's Internet Crime Complaint Center (IC3), resulting in $5.8 billion in reported losses.[2] CIF schemes are often orchestrated by Asia-based criminal syndicates, predominately operating in southeast Asia.

31. In CIF schemes, criminals contact potential victims through seemingly misdirected text messages, dating applications, or other online platforms/forums with the goal of building rapport and relationships with the victims.

[2] *See* Fed. Bureau of Investigation, Internet Crime Report 2024 at 36, https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

32. Once that trust is established, the criminal recommends virtual currency investment by touting their own, or an associate's success in the field. Investment methods vary, but a common tactic is to direct a victim to a fake investment platform hosted on a website. These websites, and the investment platforms hosted there, are created by criminals to mimic legitimate platforms. The subject usually instructs and/or assists the victim with opening an account on a centralized virtual currency exchange, such as Coinbase or Crypto.com, and then walks the victim through transferring money from a bank account to that virtual currency exchange account. Next, the victim will usually receive instructions on how to transfer their virtual currency assets to the fake investment platform. On its surface, the platform typically shows lucrative returns, encouraging further investment. However, in reality, all deposited funds are routed to a virtual currency address controlled by the criminals.

33. In CIF schemes, the subjects will continue to encourage investments until victims have depleted their savings. Oftentimes, the subject will attempt to continue the scheme by coaching victims on taking out loans against their homes or borrowing money from friends and family. Inevitably, these victims generally run out of money and make attempts to withdraw their funds. However, victims are unable to do so and are provided various excuses as to why. For example, subjects will often levy a fake "tax" requirement, stating taxes must be paid on the proceeds generated from the platform. This is just an eleventh-hour effort by subjects to elicit more money from victims; ultimately, victims are locked out of their accounts and lose all their funds. Even when victims procure enough funds to pay these "taxes," the subjects will continue to concoct new excuses and fees for victims to pay.

Initial Identified Wire Fraud Victim: R.M.

34. In or around November 2023, the FBI's San Diego field office learned of a CIF victim, R.M., who lost $626,000.

35. R.M. connected with a young female by the name of "Anna Wang" ("WANG") on Facebook in or around the summer of 2023. Shortly after R.M. and WANG began chatting, WANG requested that they move their conversation off Facebook and onto the encrypted messaging application WhatsApp, a common CIF scheme tactic. R.M. was a single father and embraced the opportunity to get to know WANG, especially after she told R.M. that she was also a single parent. The two continued to message and began to develop a romantic relationship.

36. WANG claimed to live in New York City and told R.M. that her aunt was a cryptocurrency investment expert with Goldman Sachs. WANG led R.M. to believe that, thanks to her aunt's guidance, WANG herself was very successful in investing. WANG had also expressed interest in dating R.M. but claimed that her aunt required R.M. to be financially successful in order for the aunt to allow the relationship. This served as the foundation for WANG to push R.M. into cryptocurrency investments under her guidance.

37. R.M. opened an account at the cryptocurrency exchange Crypto.com and an account through Crypto.com's mobile application "DeFi Wallet," providing R.M. with an unhosted wallet. Through DeFi Wallet's in-app browser, called a "Web3 Portal," R.M. was able to access R.M.'s aunt's purported "investment platform" called AntcCoins.com.3 WANG told R.M. that if R.M. invested $250,000, R.M. would qualify for her aunt's "VIP Level 1" portfolio which would both yield great financial returns and gain the aunt's approval for their relationship. R.M. struggled to qualify for "VIP Level 1" and was supported by WANG herself. WANG told R.M. that she would give R.M. $50,000 of her own money if R.M. could come up with the additional $200,000. Instead of sending this $50,000 to R.M. to submit, she claimed to have sent it straight into R.M.'s AntcCoins account – which immediately populated with the new balance.

38. When the account purportedly reached $250,000, achieving "VIP Level 1" status, WANG claimed her aunt reneged her offer and required R.M. to reach the "VIP Level 2" tier of $500,000 before R.M. and WANG could be in a relationship. WANG again supported R.M. by claiming to add $40,000 of her money to R.M's account. Eventually, R.M brought R.M's account balance up to $500,000.

39. R.M. ultimately received a pop-up warning message that R.M.'s account would be locked. The AntcCoins.com site administrators instructed R.M. to pay a 25% security deposit in order to withdraw R.M.'s earnings. This would equate to an additional $125,000 fee, just to withdraw R.M.'s own money.

[3] The FBI has received at least one complaint through the Internet Crime Complaint Center (IC3) referencing the site AntcCoins.com. This complaint outlined a similar scheme where the victim met a woman online, invested cryptocurrency, and was unable to withdraw their funds.

40. The FBI engages in proactive measures to identify victims actively being defrauded in CIF schemes. After the FBI identifies likely victims, it seeks to contact them and notify them that they are likely being victimized. Oftentimes, these notifications are made before the victim is aware of the scam, and thus prevents additional funds from being lost. When the FBI identified and subsequently contacted R.M., R.M. was in the process of acquiring a home equity loan to pay the 25% security deposit to access R.M.'s funds.

41. After speaking with the FBI, R.M. was unable to recover any of R.M.'s funds from this fraudulent platform and reportedly lost approximately $626,000, which severely compromised R.M.'s life's savings.

Flow of R.M.'s Funds

42. FBI special agents and forensic accountants traced portions of R.M.'s funds using reliable blockchain analysis tools in or around late November 2023. After the funds were in the scammers' possession, 41.22 ETH from R.M.'s funds were sent to and through multiple virtual currency addresses, comingling with other funds along the way. R.M.'s funds were ultimately transferred into five addresses, referred to above as the Subject Addresses. On or about December 6, 2023, Tether Ltd. froze the Subject Addresses, which held balances totaling 927,155.442 USDT. The breakdown of the USDT frozen, and later seized, balances in each of the Subject Addresses is displayed below in Table 1. The flow of funds is illustrated below in Figure 1. Virtual currency addresses are truncated for ease of reference, and all dates are on or about.

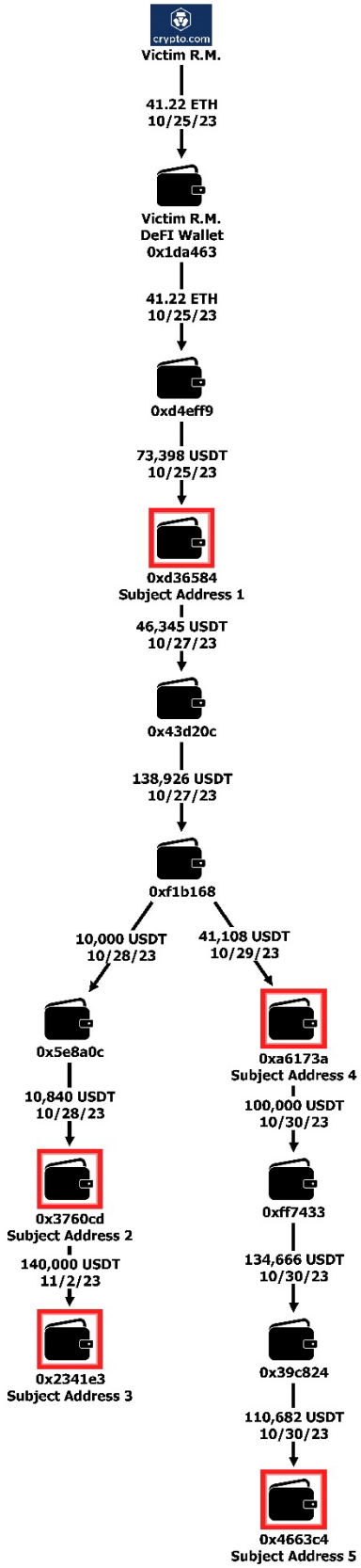

Figure 1 (above): Illustration of R.M.'s Flow of Funds to Subject Addresses

Address	Current USDT Balance
0xD365849035325A1a49bD43F5F43063F1AEC0Ccd6	31,010.63
0x3760Cd4E92F8bAe88bC4541bf5a8A5531eeA2C80	57,446.36
0x2341E30EacD99d3cB3F9b7831144C82be18157c2	200,000.00
0xa6173A4128Bb9aDEf4fBE4D858363FbcdA23c089	449,972.38
0x4663c4dF09D4dD347197507defD1551b6Ce10067	133,303.65
Total	**871,733.02**

Table 1: Subject Addresses with USDT Balances

43. As seen in Figure 1 above, the ETH that R.M. paid into the scam was laundered through numerous unhosted wallets. All of this cryptocurrency was quickly swapped to USDT. It was comingled with other funds and split down different laundering paths – essentially scattering R.M.'s funds on the blockchain, which is typically done to help conceal the location of the stolen funds. This USDT was ultimately laundered into all five SUBJECT ADDRESSES.

44. The above flow of funds (as seen in Figure 1) is indicative of money laundering using cryptocurrency, especially for CIF. At each stage above, various methods commonly used by individuals laundering money were used to frustrate law enforcement's ability to trace, and ultimately recover, any illicit proceeds. Those methods include:

- **Use of a Criminal-Proposed, Victim-Controlled Unhosted Wallet (0x1da463, Figure 1).** Criminals often coach victims to create unhosted wallets to receive victims' funds at the outset of the laundering process. In R.M.'s case, R.M. used Crypto.com's DeFi Wallet, which is now called "Onchain." The DeFi Wallet itself has its own web browser, called the Web3 portal. This portal enables users to access websites that are only available through similar portals, and not traditional web browsers, due to the sites themselves running on blockchain technology. Since victims are accessing the malicious investment websites within the Web3 portal,

they are left with the impression that they are investing their cryptocurrency in the unhosted wallet itself. This was the case with R.M., where R.M. accessed AntcCoins.com through DeFi Wallet and initially believed that Crypto.com was the party withholding R.M.'s funds, because DeFi Wallet is a Crypto.com product. Criminals coaching victims on depositing funds into these unhosted wallets to then send to them through fraudulent investment platforms provides an additional barrier, where law enforcement cannot easily access the malicious platforms and where victims cannot easily identify the scam.

- **Use of Unattributable "0-Level" Deposit Addresses (0xd4eff9, Figure 1).** 0-Level addresses are the initial deposit addresses that CIF scammers provide victims to deposit their funds on the blockchain. Criminals usually provide 0-Level addresses associated with unhosted wallets to evade identification or potential interference by third parties. Such is the case here with 0xd4eff9. These 0-Level addresses are oftentimes only shared with one victim to make it more difficult for law enforcement and others to track and report common scams.
- **Use of Decentralized Exchanges (0xd4eff9, Figure 1**). DEXs allow users to swap one cryptocurrency type for another, often without having to provide any identifying information (i.e., know your customer ("KYC") data)), so users can remain anonymous. R.M.'s funds were swapped from ETH to USDT using a DEX.
- **Swapping for Stablecoins, Especially USDT (0xd4eff9, Figure 1).** CIF scammers involved in laundering victims' funds regularly exchange or "swap" the non-stablecoin cryptocurrencies that victims send them for stablecoins, especially USDT**.** According to investigators, money launderers are particularly drawn to

USDT because of its low transactions fees and stability compared to other more volatile cryptocurrencies. Additionally, USDT is compatible on several different blockchains, which makes it easier to move funds across blockchains to further obfuscate the nature, source, control, and/or ownership of criminal proceeds.

- **High Velocity Flow of Funds to Consolidation Wallet**. **(0xd4eff9, 0x43d20c, 0x5e8a0c, 0xff7433 Figure 1).** Once deposited into the 0-Level Address, it is common for funds to be transferred quickly from address to address before reaching the consolidation wallet, where the funds will often rest for a longer period, allowing criminals time to comingle those funds with other illicit gains before moving the funds again from the consolidation wallet towards a cash-out point where they can convert the pool of funds to fiat currency. R.M.'s funds reflect this method on numerous occasions by being transferred into, and out of, addresses within minutes.
- **Use of Consolidation Wallet to Comingle Funds. (0xf1b168c, Figure 1)** Defined as the "layering" stage of money-laundering, funds derived from multiple victims are routed to the same address, where they are comingled, consolidated, and transferred together downstream. Criminals use consolidation wallets to obfuscate the source of funds and complicate tracing efforts by investigators. R.M.'s funds were comingled at almost every step, and ultimately passed through multiple consolidation wallets containing other victims' funds before being sent to, or passing through, the Subject Addresses 2, 3, 4, and 5.

45. There is no reason, economic or otherwise, for legitimate businesses or individuals to conduct cryptocurrency transfers using all of these methods. Whether transferring BTC or, in this case, ETH and USDT, each individual cryptocurrency transfer costs money. For USDT, that cost comes through the payment of transactions fees, or "gas" fees, required by the Ethereum blockchain. It is reasonable to assume that businesses and individuals would strive to minimize those fees by conducting transfers with as few transactions, or "hops," as possible. Furthermore, each transaction delays the whole process, defeating one of the key attributes of cryptocurrency as a quick means of exchange.

46. Based on this evidence, and additional evidence outlined below, unknown subjects orchestrated a criminal CIF scheme against R.M. and laundered R.M.'s funds, and funds of other victims, into the Subject Addresses.[4]

Identification Of Additional Victims

47. The FBI performed blockchain analysis to trace transactions backwards from the Subject Addresses to eventually identify other 0-Level addresses not shown in Figure 1. It was determined that these 0-Level addresses received deposits from multiple wallets hosted at the virtual currency exchanges Coinbase, Kraken, and Crypto.com. Investigators sent legal process to the exchanges to identify likely victim account holders.

[4] While all Subject Addresses received funds from R.M. and other identified victims, only Subject Address 3 was identified as holding R.M.'s funds at the same time it was holding other identified victims' funds.

48. By reviewing records from Coinbase, Kraken, and Crypto.com, complaints submitted to the IC3, and subsequent interviews with identified exchange account holders, investigators confirmed that the Subject Addresses contained additional victim proceeds. Specifically, victims with initials B.M., A.B., E.H., W.H., E.F., D.H., P.B., R.K., V.S., S.S., S.I. and N.R., sent funds to 0-Level addresses, which were ultimately transferred to the Subject Addresses. The flow of these victims' funds into the Subject Addresses is shown below in Figure 2. All dates are approximate.

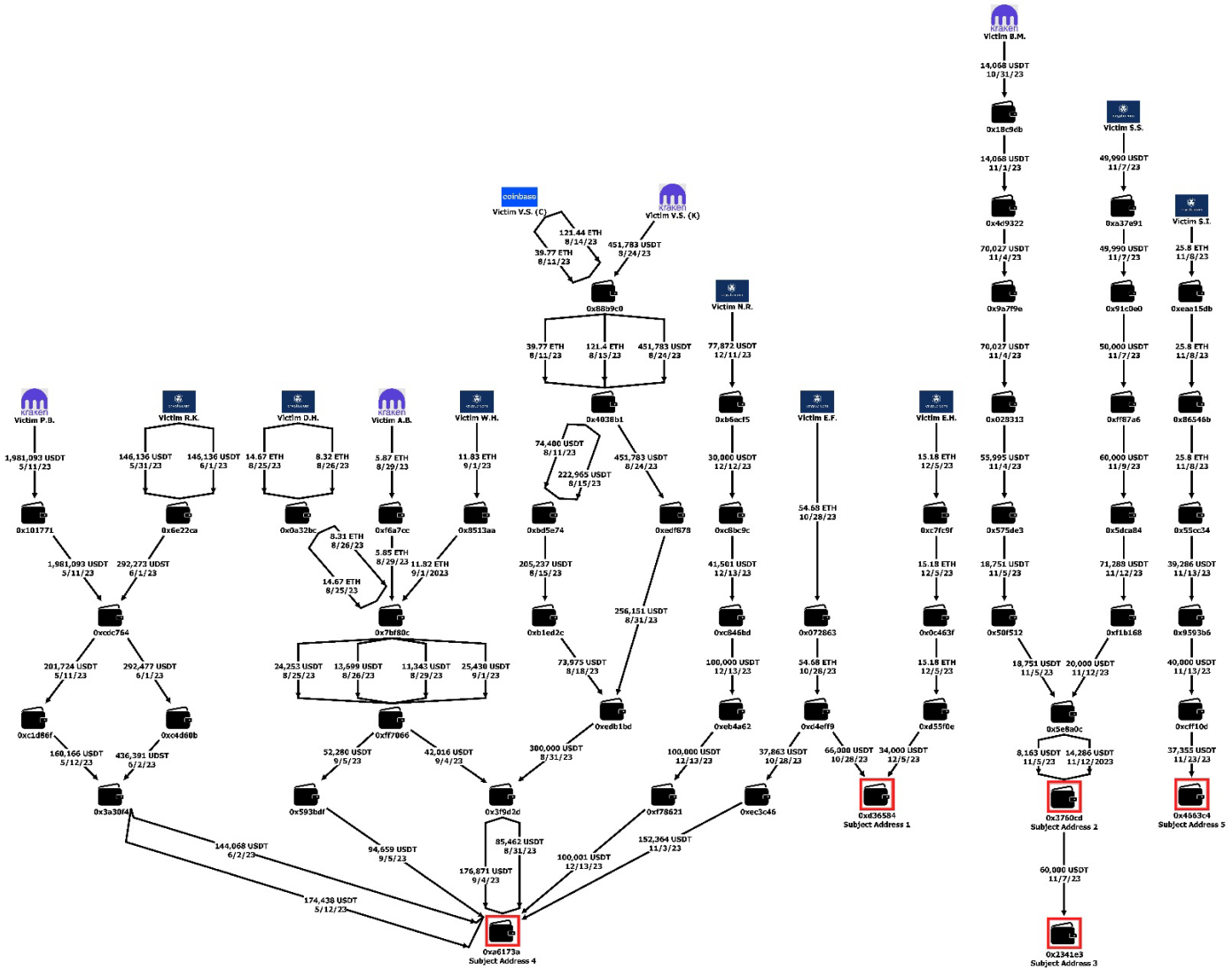

Figure 2 (above): Illustration of Flow of Funds from Additional Victims to Subject Addresses

49. Similar to R.M., victims E.H. and E.F. met someone online who directed them to invest in the fake investment platform AntcCoin.com.[5] E.H. also accessed this platform through an unhosted wallet's Web3 portal. After becoming suspicious of AntcCoin.com, E.H. attempted a withdrawal, which was never processed. After this attempt, E.H.'s AntcCoin.com account supposedly received an unexpected $600,000 deposit, which resulted in E.H.'s account being "frozen." AntcCoin.com claimed that E.H.'s account was involved in money laundering and required E.H. to pay $15,000 to unfreeze E.H.'s account, which E.H. did not pay. In total, E.H. reportedly invested approximately $90,000 and has been unable to recover any of E.H's investment.

50. E.F. met a woman on Facebook who encouraged E.F. to reach a minimum investment threshold of $500,000. The woman offered to "invest" some of her own money to help E.F. meet this threshold. Upon reaching this investment threshold, E.F. was told that the tier had been raised to $600,000. E.F. eventually attempted a sizable withdrawal, which resulted in E.F.'s AntcCoin.com account being "frozen." The investment platform claimed that E.F.'s account was flagged for money laundering and instructed E.F. to pay a fee of $45,000. Later, AntcCoin.com demanded that E.F. pay 30% of E.F.'s account balance to process any withdrawals. In total, E.F. reportedly invested approximately $223,000 and has been unable to recover any of E.F.'s investment.

51. Part way through E.F.'s investments with AntcCoin.com, the site told E.F. that it was under maintenance and transitioning to AntcData.com. At one point, the woman from Facebook accidently "pocket dialed" E.F. During this, E.F. could hear what sounded like three men talking in a foreign language before realizing the phone was on and hung up.

[5] AntcCoin, similar to the AntcCoins.com that R.M. was victimized, has been referenced in at least one IC3 complaint.

52. Victims B.M., D.H., and N.R. were initially contacted through a dating website. The scammers requested to communicate through WhatsApp, where they developed the trust of the victims and coaxed them into signing up for fake cryptocurrency investment platforms. B.M. met a woman on the dating application Plenty of Fish and was directed to the fake investment platform PPBVTZI.vip. B.M. ultimately invested approximately $80,000. When B.M. attempted to withdraw B.M.'s money, the site's customer service team told B.M. that no withdrawals were allowed until B.M. deposited a total of $150,000. B.M. immediately grew suspicious and noticed inconsistencies in the WhatsApp messages of the woman. B.M. was unable to recover any of B.M.'s investment.

53. D.H. met a woman on the dating site Facebook Dating and was directed to the fake investment platform EDX-markets.net.[6] D.H. had invested over $150,000 and was only able to make four small withdrawals of about $2,000. Eventually, D.H. attempted to withdraw $10,000, which did not go through. The woman D.H. met on Facebook Dating, despite not claiming to work for EDX-martkets.net, somehow knew D.H. made this withdrawal attempt and told D.H. to cancel it. D.H. has not been able to withdraw anything additional and has found reviews online that claim EDX-markets.net is associated with scams.

[6] EDX-markets.net have been referenced in at least six IC3 complaints

54. N.R. met a woman on a dating website and was directed to a cryptocurrency investment platform. N.R. had been investing on the platform for a while before being emailed by an unknown person who alerted N.R. to the scam. This person warned N.R. against continuing investments and claimed that they had been forced to scam people like N.R. While N.R. was unable to verify who the unknown person was, N.R. did immediately make withdrawal attempts that were met with a massive request for taxes. At this point, N.R. realized the platform was indeed a scam and since then has been unable to get any of N.R.'s money out. In total, N.R. reportedly invested approximately $400,000.

55. Victims A.B., W.H., R.K., V.S., S.S., and S.I., were initially contacted through social media. The scammers requested to communicate through WhatsApp, where they developed the trust of the victims and coaxed them into signing up for fake cryptocurrency investment platforms.

56. A.B. met a woman on Facebook and was directed to the investment group Myth.Market. A.B. ultimately invested approximately $156,000. $75,000 of this total investment was procured through a loan that A.B. was attempting to repay. When A.B. attempted to withdraw profits to pay off this loan, Myth.Market claimed that A.B.'s account at the cryptocurrency exchange Coinbase had been flagged and frozen as suspicious. Myth.Market told A.B. that A.B. needed to pay a verification fee of $240,000 to have A.B.'s funds released. A.B. then recognized this was a scam and has been unable to recover A.B.'s investment.

57. W.H. met a woman on Facebook and was directed to the fake investment platform EDX-markets.net. W.H. had invested a significant amount in the platform and had been unable to recover any of W.H.'s investments. W.H. suffers from cognitive decline and reviewed the situation with W.H.'s daughter who took over after realizing this was a scam. The daughter contacted a private investigator who determined that the images used by the Facebook woman had been stolen from the social media account of a model.

58. R.K. was contacted by a woman on Facebook whose name resembled someone R.K. knew from long ago. R.K. was directed to the fake investment platform Coinrule-web3.shop. R.K. made two attempts to withdraw money from R.K.'s platform account. At first, the scammers claimed that R.K. money was under a probationary period and withdrawals were not yet allowed. Later, R.K. was told that the withdrawal could not be processed because R.K. was being investigated by the SEC. In total, R.K. reportedly invested approximately $608,000 and has been unable to recover R.K.'s investment.

59. V.S. met two women on LinkedIn who directed V.S. to the fake investment platforms "IFCDEX" and "Toobitrac".[7] V.S. had successfully made small withdrawals early on but has since been unable to recover any additional amounts from V.S.'s "investments." In total, V.S. invested approximately $1,100,000.

60. S.S. met a woman on Facebook who directed S.S. to the fake investment platforms Dyd-x.com and web3-ethereum.io. S.S. had been investing for a while before receiving a call from the FBI notifying S.S. that S.S. was a victim of CIF. After receiving this call, S.S. attempted to withdraw $500,000. This was rejected and a request for taxes followed, just as the FBI had warned. In total, S.S. reportedly invested about $450,700 and has been unable to withdraw anything.

[7] Toobitrac has been referenced in at least three IC3 complaints.

61. S.I. met a woman on LinkedIn who directed S.I. to a cryptocurrency investment platform. S.I. invested approximately $250,000 and has been unable to withdraw anything. When S.I. attempted to make withdrawals, S.I. was directed to pay $40,800 for "blockchain services." After paying this, the scammers claimed that S.I. was 27 days late and needed to pay $275,400 in late fees. After consultation with S.I.'s family, S.I. realized S.I. had been scammed.

62. Victim P.B. reportedly met a woman on a plane who stayed in touch with P.B. She eventually introduced P.B. to the fake investment platform Coinrule-web3.8. P.B. withdrew money from P.B.'s retirement accounts to invest in this opportunity. After P.B. stopped investing, the platform told P.B. that if P.B. did not send more money, P.B. would be fined $230,000. In total, P.B. reportedly invested $10 million and has not recovered any of P.B.'s funds.

63. Table 2, displayed below, outlines the approximate known loss amounts reported by the listed identified victims whose funds were traced to the Subject Addresses. Note that not all values take into account the initial minimal amounts that victims may have been able to withdraw before they were ultimately blocked from making any additional withdrawals, due to the FBI not knowing and/or being able to confirm the value of these withdrawals.

[8] Coinrule-Web3 has been referenced in at least 12 IC3 complaints.

Victim	Total Loss Amount
R.M.	$ 626,000.00
B.M.	$ 80,000.00
A.B.	$ 156,000.00
E.H.	$ 90,000.00
W.H.	$ 66,155.00
E.F.	$ 223,000.00
D.H.	$ 150,000.00
P.B.	$ 10,000,000.00
R.K.	$ 608,516.00
V.S.	$ 1,100,000.00
S.S.	$ 450,700.00
S.I.	$ 249,440.00
N.R.	$ 400,000.00
Total	$ 14,199,811.00

Table 2 (see above): Summary of Total Reported Victim Loss Amounts

Analysis of Subject Addresses

64. As outlined below, the FBI used reliable blockchain analytics tools to review the Subject Addresses' activity, patterns, and associations with other known scams. According to investigators, all Subject Addresses' activity was highly indicative of the type of money laundering often seen when investigating the transfer of CIF proceeds. As further discussed below, all balances are based upon amounts of USDT that Tether indicated to have frozen.

65. Table 3, displayed below, provides an overview of the amount of identified victims' funds that have been directly traced into the Subject Addresses.

Subject Address	Associated Victims	Amount of Victim Funds Traced To Subject Address
1	R.M., E.H., E.F.	$ 178,398.00
2	S.S., R.M., B.M.	$ 32,449.00
3	R.M., B.M.	$ 18,163.00
4	N.R., R.M., P.B., A.B., W.H., E.F., D.H., R.K., V.S.	$ 552,958.04
5	R.M., S.I.	$ 60,012.41

Table 3 (see above): Summary of Subject Addresses and Associated Victim Funds Traced to Subject Addresses

Subject Address 1:

66. Subject Address 1 held a balance of 31,010.63 USDT. 178,398 in USDT from three identified victims has been traced into the address. Although most of those funds were moved to other addresses, 23,000 USDT in identified victim funds remained in the address once it was frozen, commingled with funds of yet unidentified transferor origins.

67. Subject Address 1 received primarily deposits of USDT, which is commonly used in CIF schemes. Using a reliable blockchain analytics tool, investigators determined that most of the funds received by this address came through a decentralized exchange, used by the launderer(s) to swap ETH for USDT. The use of a decentralized exchange, including to exchange one type of virtual currency for another, is a common technique used to launder CIF proceeds.

68. The launderer(s) sent identified victim funds to Subject Address 1 on or about the same day as they were received from the victim, after the funds passed through at least one intermediary address. According to investigators, this rapid movement of funds received from victims is used by cryptocurrency launderers for obfuscation purposes.

69. Analysis of the funds sent from SUBJECT ADDRESS 1 indicated that a majority of these funds were eventually sent to virtual currency exchanges, such as Binance or OKX.

70. As seen in Figure 1, Subject Address 1 also served as an intermediary address for R.M.'s funds, before the funds were ultimately sent to and through the other Subject Addresses.

Subject Address 2

71. Subject Address 2 held a balance of 57,446.36 USDT. 32,449 in USDT from three victims has been traced into the address. 14,286 USDT in identified victim funds remained in the address after it was frozen, commingled with funds of unidentified transferor origins.

72. Subject Address 2 primarily received deposits of USDT, which is commonly used in CIF schemes. A majority of the funds received by this address came through a decentralized exchange, used by the launderer(s) to swap ETH to USDT, while remaining anonymous. The use of a decentralized exchange, especially to swap a non-stablecoin cryptocurrency (like ETH) to a stablecoin (like USDT) is another technique commonly used to launder CIF proceeds.

73. Identified victim funds were sent through multiple intermediary addresses, all within approximately three to five days between the funds being sent by victims and ultimately deposited into Subject Address 2. All identified victim funds passed through the same consolidation address before reaching Subject Address 2. According to investigators, this quick movement of victim funds through multiple intermediary unhosted wallet addresses, and their commingling in a consolidation address, is commonly used by cryptocurrency launderers to disguise the nature, source, location, ownership, and control of victim funds.

74. A majority of the funds sent from Subject Address 2 went to other unhosted wallet addresses, including Subject Address 3, and eventually were sent to either virtual currency exchanges, such as Binance or OKX, or decentralized exchanges.

75. Additionally, investigators reviewed information from a reliable blockchain analysis tool that indicated Subject Address 2 had received virtual currency from multiple scams. The company that manages this tool has an internal investigation team that manually reviews and flags suspicious blockchain activity. They utilize open-source information and have their own fraud reporting platform to assist them in identifying malicious actors. The tool marked numerous inflows as associated with scams under the website associated names aceqbxz.top, coinrule-web3.bid, foxwallet.cyou, and foundypro.net, as well as "Pig Butchering Syndicate 1."[9] This tool also marked numerous inflows as associated with submitted community complaints, to include those linked to the domains ngstruart.com and ngstruart.pro.[10]

Subject Address 3:

76. Subject Address 3 held a balance of 200,000 USDT. 18,163 in USDT from two victims has been traced into the address, which remained in the address after it was frozen, commingled with funds of yet unidentified transferor origins.

77. Subject Address 3 only received two deposits of USDT, both from Subject Address 2. Most of the funds received by Subject Address 3 came from centralized exchanges Kraken.com and Crypto.com and a decentralized exchange. This address had not transferred funds out prior to being frozen.

Subject Address 4:

[9] IC3 has received at least one complaint referencing coinrule-web3.bid and at least two complaints referencing foxwallet.cyou.

[10] IC3 has received at least three complaints referencing ngstruart.com and at least seven complaints referencing ngstruart.pro.

78. Subject Address 4 held a balance of 449,972.38 USDT. 552,958.04 in USDT from nine victims has been traced into the address. 30,000 USDT in identified victim funds remained in the address after it was frozen, commingled with funds of unidentified transferor origins.

79. Subject Address 4 primarily received deposits of USDT. A majority of the funds received by this address came from centralized exchanges. Investigators reviewed information from a reliable blockchain analysis tool that indicated that this address had received cryptocurrency from addresses associated with multiple scams, such as the reported scam domains oktexk.com, nft-uniswap.net, bitviropro.com, and many more.[11] This tool also flagged incoming transfers to this address that were related to community complaints.

80. Figure 2 illustrates the multiple laundering chains that feed into Subject Address 4, which served as a consolidation address for multiple identified victims' funds.

81. During 2023, Subject Address 4 received over 77,000,000 USDT via 534 transactions, with an average transaction amount of approximately 144,443 USDT. This address sent over 76 million USDT via 818 transactions, with an average transaction amount of approximately 93,744 USDT. It also transacted with 301 different addresses, the majority of which were involved in only one or two total transactions. Subject Address 4 would receive deposits and then almost completely empty out, transferring nearly all funds elsewhere. A non-commercial entity conducting this quantity of transactions, with these many different addresses, cannot be reasonably explained as engaging in legitimate activity and indicates that the address is part of a large-scale money laundering network.

[11] IC3 has received at least one complaint referencing oktexk.com, at least six complaints referencing nft-uniswap.net, and at least seven complaints referencing bitviropro.com.

82. A majority of the funds sent from Subject Address 4 were eventually sent to centralized virtual currency exchanges, such as Binance or OKX. This address also used a decentralized exchange multiple times to swap cryptocurrencies. According to information obtained from a reliable blockchain analytics tool, Subject Address 4 had over 100 instances where its deposits flowed into U.S.-sanctioned and then-U.S.-sanctioned virtual currency exchanges, the Iranian exchange Nobitex, and to addresses associated with the Democratic People's Republic of Korea.

Subject Address 5:

83. Subject Address 5 held a balance of 133,303.65 USDT. 60,012.41 in USDT from two victims has been traced into the address. 23,667.41 USDT in identified victim funds remained in the address after being frozen, commingled with funds of unidentified transferor origins.

84. Subject Address 5 primarily received deposits of USDT, which is commonly used in CIF schemes and their laundering of proceeds. As displayed in Figures 1 and 2, funds from victims R.M. and S.I. went through multiple intermediary addresses between victims' deposits and Subject Address 5.

85. Using a reliable blockchain analytics tool, investigators determined that the primary source of funds received by this address originally came from centralized exchanges, including Kraken and Crypto.com. This tool also provided information that this address has received virtual currency from addresses associated with multiple scams including scams associated with sichcapitalsd.com, gateexproq.com, bitmart-trust.com, and kyolo.net, as well as various addresses the tool marked as a "Pig Butchering Grouping."[12] Similar to Subject Address 4, this address had multiple withdrawals where its outgoing funds were sent to addresses marked by the blockhain analytics tool as scams, sanctioned entities, or flagged in community complaints. A majority of the funds sent from Subject Address 5 were eventually sent to centralized virtual currency exchanges, such as Binance or OKX.

Claimant Of Subject Addresses

86. The Subject Addresses are all unhosted wallet addresses where the owners cannot be easily identified. Pursuant to a law enforcement request, Tether Ltd. froze the USDT associated with the Subject Addresses. Following the freeze, Tether Ltd. was contacted by claimants for Subject Addresses 2 and 4.

[12] IC3 has received at least one complaint referencing sichcapitalsd.com, fourteen complaints referencing gateexproq.com, two complaints referencing bitmart-trust.com, and nine complaints referencing kyolo.net.

87. On or about January 9, 2024, Tether Ltd. alerted investigators that an individual had contacted them claiming ownership of Subject Address 2. Tether added that the person messaged them from the email address guoguoguoguoji@gmail.com under the name and alias "mark." Tether referred "mark" to contact the FBI via email. Investigators never received a message from this email address but on or about January 14, 2024, investigators received a message from the email address kem101299@hotmail.com using the name Mark, in Chinese characters. Mark inquired why the funds were frozen within this address. On or about January 17, 2024, investigators responded with a list of questions for Mark to self-identify and explain the use of this address. Investigators never received a response.

88. On or about December 15, 2023, Tether Ltd. alerted investigators that they received an email from cloud201291@gmail.com using the name and alias "DavidLi" regarding Subject Address 4. DavidLi stated to Tether Ltd. that Subject Address 4 "had been used normally and would like to know the reason [for the freeze]." Tether Ltd. referred DavidLi to contact the FBI via email. On or about December 18, 2023, investigators received a message from the same email address under the name "Jhay." Jhay claimed that he did not know why the account was frozen and asked investigators to contact him if he needed to provide any information. On or about December 20, 2023, investigators responded with a list of questions for Jhay to self-identify and explain the use of this address. Investigators never received a response.

89. On or about December 22, 2023, Tether Ltd. alerted investigators that they received an email from m67074603@icloud.com under the name and alias "Mr.Lin" regarding Subject Address 4. Tether Ltd. referred Mr.Lin to contact the FBI via email. On or about December 23, 2023, investigators received a message from the same email address under the name "Huiru Lin." Investigators responded with a list of questions to give Lin an opportunity to self-identify and explain the use of the address. Lin and investigators exchanged several messages where Lin answered some questions while avoiding others, despite investigators repeatedly inquiring.

90. Lin claimed to be a "freelancer, engaged in digital currency related trading activities." Lin claimed that there was no record of communications with his clients because the business was conducted in-person. Investigators sent Lin a list of ten transactions flowing into Subject Address 4 and asked him to identify the associated clients and source of funds. Of these ten transactions, two came from the same virtual currency address. Lin provided scanned copies of ten different Chinese nationals' identification (ID) cards.

91. After further inquiry from Lin, investigators asked about the withdrawals from Subject Address 4 associated with the same ten transactions above. While Lin continued to respond, he did not provide answers to most questions from investigators. At one point, Lin wrote that his buying and selling of cryptocurrency is "more of a secret operation" and that the USDT cryptocurrency had "not yet been established in China. Allowed." Investigators continued to give Lin opportunities to respond to unanswered requests, such as providing a readable scan of his own identification card and his mailing address, but Lin has not responded.

COUNT ONE – FORFEITURE OF DEFENDANT PROPERTY

(18 U.S.C. § 981(a)(1)(C))

92. 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.

93. 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))

94. The Defendant Property constitutes property involved (a) domestic and international concealment of money laundering transactions committed in violation of Title 18, United States Code, Sections 1956(a)(1)(B)(i) and 1956(a)(2)(B)(i), (b) a conspiracy to engage in money laundering, committed in violation of Title 18, United States Code, Section 1956(h).

95. Accordingly, the Defendant Funds are 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.

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, Charles Linnerooth, 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 13 th day of November 2025.

Charles Linnerooth

Charles Linnerooth
Special Agent
Federal Bureau of Investigation