CRAIG H. MISSAKIAN (CABN 125202)
United States Attorney

MARTHA BOERSCH (CABN 126569)
Chief, Criminal Division

DANIEL PASTOR (CABN 297948)
Assistant United States Attorney

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
Telephone: (415) 436-7230
FAX: (415) 436-7234
daniel.pastor@usdoj.gov

Attorneys for United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. APPROXIMATELY 1,288,389.76 USDT FROM TRON BLOCKCHAIN ADDRESS Defendant.	CASE NO. **VERIFIED COMPLAINT FOR CIVIL FORFEITURE IN REM**

The United States of America, through its attorneys Craig H. Missakian, United States Attorney for the Northern District of California, and Daniel Pastor, Assistant United States Attorney, brings this complaint and alleges as follows:

NATURE OF THE ACTION

1. This is a judicial forfeiture action in rem, as authorized by Title 18, United States Code, Sections 981 and 983.

2. This Court has jurisdiction under Title 18, United States Code, Section 981, and Title 28, United States Code, Sections 1345 and 1355, as the defendant property constitutes or is derived from proceeds obtained, directly or indirectly, from violations of Title 18, United States Code, Sections 1343, 1349, and 1956, as well as property involved in violations of Title 18, United States Code, Section 1956.

3. This action is timely filed in accordance with Title 18, United States Code, Section 983.

4. Venue is proper because the defendant property represents the proceeds of a crime that may be prosecuted in the Northern District of California. 28 U.S.C. §§ 1355, 1395.

5. Intra-district venue is proper in the San Francisco division within the Northern District of California.

PARTIES

6. Plaintiff is the United States of America.

7. The **Defendant Property consists of 1,288,389.76 USDT** seized from Tron blockchain address TEZRLkhrWADL4LemEMHv25hnGK935GYzh4 (**Subject Wallet Address**).

FORFEITURE STATUES

8. Wire fraud forfeiture: Title 18, United States Code, Section 981(a)(1)(C) provides that "[a]ny property, real or personal, which constitutes or is derived from proceeds traceable" to the violation of an enumerated statute constituting a specified unlawful activity "is subject to forfeiture to the United States." Specified unlawful activities are detailed therein, as well as in Title 18, United States Code, Sections 1956(c)(7) and 1961(1), which enumerates Title 18, United States Code, Sections 1343 and 1349 as specified unlawful activity. This section provides both civil forfeiture authority and criminal forfeiture authority by virtue of Title 28, United States Code, Section 2461(c).

9. Money laundering forfeiture: Title 18, United States Code, Section 981(a)(1)(A) provides for the civil forfeiture of any property, real or personal, that is involved in a transaction or attempted transaction in violation Title 18, United States Code, Sections 1956, 1957, or 1960, or any property traceable to such property. Title 18, United States Code, Section 982(a)(1) provides for the criminal forfeiture of any property, real or personal, that is involved in a transaction or attempted transaction in

violation Title 18, United States Code, Sections 1956, 1957, or 1960, or any property traceable to such property.

10. One of the chief goals of forfeiture is to remove the profit from crime by separating the criminal from his or her dishonest gains, and to divest criminal actors from the apparatus allowing them to engage in criminal activity. *See United States v. Newman*, 659 F.3d 1235, 1242 (9th Cir. 2011); *United States v. Casey*, 444 F.3d 1071, 1073 (9th Cir. 2006).

11. In cases involving a money laundering offense, the forfeiture statutes connected to money laundering offenses permit the government to forfeit property "involved in" money laundering. Such property includes "untainted property" commingled with "tainted" property, when that untainted property is used to facilitate the laundering offense, such as by obscuring the nature, source, location, or control of any criminally derived property. See Title 18, United States Code, Sections 981(a)(1)(A), 982(a)(1); *see also United States v. Kivanc*, 714 F.3d 782, 794-95 (4th Cir. 2013); *United States v. Huber*, 404 F.3d 1047, 1056-1058 (8th Cir. 2005).

BACKGROUND ON VIRTUAL CURRENCY

12. 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.

13. Cryptocurrencies, like USDT, Ether, or Tronix, 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.

14. A cryptocurrency 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.

15. A virtual currency 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.

16. 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.

17. An unhosted wallet—also known as a self-hosted or 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.

18. Many virtual currencies publicly record their transactions on what is known as a 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 the known balances for each virtual currency address on the blockchain.

19. 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.

20. A cryptocurrency exchange—is a platform used to buy and sell cryptocurrencies. Cryptocurrency exchanges allow users to exchange their cryptocurrency for other virtual currencies or fiat currency, and vice versa. Many exchanges also store their customers' cryptocurrency addresses in hosted wallets. Exchanges like Coinbase or Kraken are centralized, meaning that they facilitate virtual currency trading between parties on a large scale and often resembles traditional asset exchanges like a stock exchange. Exchanges can also be decentralized, meaning that they are peer-to-peer marketplaces where transactions occur directly between parties.

21. Stablecoins are a type of virtual currency whose value is pegged to a commodity's price, such as gold, or to a fiat currency, such as the U.S. dollar, or to a different virtual currency. For example, USDT is a stablecoin pegged to the U.S. dollar at a roughly 1:1 ratio.

22. Tether Limited ("Tether") is the company that manages the smart contracts and the treasury (i.e., the funds held in reserve) for USDT tokens. Ether is the native cryptocurrency on the Ethereum network (the name for the Ethereum blockchain). Tronix (TRX) is the native cryptocurrency of the Tron blockchain.

BACKGROUND ON CRYPTOCURRENCY INVESTMENT FRAUD SCHEMES

23. The wire fraud and money laundering offenses described in this affidavit occurred as part of cryptocurrency investment fraud (CIF) schemes. CIF schemes, commonly referred to as "pig butchering," generally involve scammers tricking consumer victims into making purported "investments" in virtual currency on fraudulent or non-existent investment platforms, typically alleged to be managed by a third-party, and providing fictitious returns to encourage additional investments.

24. The scammers typically initiate contact with victims through social media platforms and form a relationship with the victim to gain the victim's trust. Those relationships may be perceived by the victims as romantic, professional, or friendship based. The scammers often create profiles using fictitious names, locations, images, and personas, allowing the scammers to cultivate perceived personal relationships with prospective victims.

25. Once the scammers develop a rapport with the victim, they will often introduce the victim to cryptocurrency and to at least one fraudulent investment platform through which the victim can

"invest". The scammers promise a lucrative return if the victim invests, as the scammers allegedly he/she has obtained, on the fake third-party platform. Scammers manipulate the fraudulent investment platform to show an increase in the victim's account balance. The scammers often provide falsified transaction records or photos that depict the scammers contributing their own funds to the victim's initial investment.

26. Enticed by the falsified returns, victims continue to invest, until they try to retrieve their gains, only to find that they are unable to retrieve them. The scammers then demand that victims make additional payments to the platform for their investments to be released and/or withdrawn. Examples include, victims being required to pay an additional percentage to the fraudulent platform to purportedly guarantee the funds, prepay taxes on the balance, or pay a fee/fine due to suspicious money laundering activities. Eventually, scammers complete their theft once they believe they are unlikely to extract any more funds from the victim, and usually cease contact with the victim, never providing the return of the victim's "invested" funds.

27. Based on agents' knowledge and experience, agents know that cryptocurrency investment scam compounds, from which workers target victims, are generally based in Southeast Asia; however, scam compounds have recently expanded to other continents. Criminal organizations run these compounds and often use forced labor victims to carry out CIF schemes.

28. Perpetrators of CIF schemes are highly effective in gaining an individual's trust and/or affection in a short amount of time using manipulative tactics and language. A single scheme is often facilitated by multiple individuals with different roles and responsibilities, including registrants, developers, and operators of these online platforms. Criminal syndicates involved in CIF schemes commingle, consolidate, and coordinate their post-fraud money laundering activities of illicitly obtained victim proceeds.

29. According to the 2024 FBI Internet Crime Report, in 2024, 41,557 cryptocurrency investment complaints were submitted, alleging $5.8 billion in losses.[1]

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

30. U.S. law enforcement frequently performs cryptocurrency tracing (blockchain tracing) to investigate CIF schemes and to locate victims' funds. Investigators often find evidence preserved on various blockchains used by criminals to move the funds, which indicates how the victim funds were acquired and where the funds were sent.

31. The process of cryptocurrency tracing and attempting to retrieve victim funds often involves following funds from their point of origin (e.g., a victim's account with a cryptocurrency currency exchange such as Coinbase or a victim-controlled wallet) to a destination at which law enforcement can attempt to seize the funds.

32. Law enforcement typically works collaboratively with cryptocurrency exchanges and stablecoin issuers to freeze criminal proceeds so that the cryptocurrency remains available for seizure, forfeiture, and the return of funds to victims.

FACTS

The Wire Fraud (CIF) Scheme and Victim-1

33. The FBI initiated an investigation based on a fraud complaint made to the FBI San Francisco Field Office by Victim-1, a 60-year-old resident of Larkspur, California.

34. Around November 2024, Victim-1 was tricked and cheated in a CIF scheme and lost a total of roughly $2.5 million in cryptocurrency.

35. Around October 2024, Victim-1 received a message on the dating application, "Elite Singles," from a woman purportedly named Olivia Leroy ("Olivia").

36. After exchanging multiple messages through the dating application, Olivia suggested that the two continue their conversation on WhatsApp.

37. Victim-1 and Olivia chatted on WhatsApp beginning on or about November 1, 2024. Olivia supposedly lived in Burlingame, California, where she claimed to work as a senior investment analyst at Goldman Sachs.

38. Olivia sent photos of herself to Victim-1 through WhatsApp while they were getting to know each other romantically.

39. The FBI received the photo of "Olivia" shown below from Victim-1.

40. Olivia told Victim-1 that she was very successful with "money to burn." They exchanged messages over WhatsApp where they discussed their interests and their hopes and dreams. For example, they discussed retiring to Hawaii together.

41. Olivia built Victim-1's trust and told Victim-1 personal details about how she was cheated on in the past, which she claimed had made her very shy and guarded. Olivia used this excuse to avoid video chatting with Victim-1.

42. After a few weeks of their online-only relationship, Olivia encouraged Victim-1 to set up a cryptocurrency wallet and to begin investing in cryptocurrency.

43. Victim-1 was not familiar with cryptocurrency, but Olivia assured Victim-1 that she would walk him through the process. Olivia stressed the importance of keeping his wallet secure and told him not to share his seed phrase[2] with anyone.

44. Olivia encouraged Victim-1 to send screenshots throughout the process so she could ensure he did not make any mistakes. Olivia's concern about how Victim-1 secured his funds helped Olivia gain Victim-1's trust.

45. After Victim-1 purchased Bitcoin using his Trust Wallet, Olivia guided Victim-1 through his first trade on or about November 6, 2024.

46. Olivia also directed Victim-1 to use the website, "www.blokcainice.com", which was where Olivia first introduced Victim-1 to cryptocurrency investing. Victim-1 was only able to invest

[2] A seed phrase generally serves as a virtual currency wallet recovery password.

about $1,000 before the website shut down, which Olivia criticized profusely.

47. Victim-1 was initially purchasing cryptocurrency to use for investing purposes through "Strike,"[3] but on or about November 7, 2024, Olivia encouraged Victim-1 to switch to using the cryptocurrency exchange Coinbase for speedier transactions with lower fees.

48. Olivia then instructed Victim-1 on how to download Blockdcgchain through Trust Wallet and told him via WhatsApp that Blockdcgchain was the trading platform that she recommended.

49. Olivia sent Victim-1 screenshots circling the buttons he needed to click and how to link his wallet to send funds to Blockdcgchain.

50. Victim-1 visited the cryptocurrency platform Blockdcgchain and watched his purported balance grow steadily. The balance increased with Victim-1's balance at one time showing $38 million on the platform.

51. The rapid increase in Victim-1's balance led him to believe he was earning a high return on every dollar invested. Victim-1 accessed the Blockdcgchain platform through his Trust Wallet app. Victim-1 started by investing smaller amounts, but as time passed and his trust in Olivia grew, he invested larger sums of money with transactions ranging from approximately $400,000 to approximately $1 million worth of cryptocurrency.

52. FBI agents know from experience that a common ploy in CIF scams is for scammers to provide a victim with access to a fake online investment account which the victim can review in real time. Victims will often continue to transfer money to these platforms that they believe are secure investment accounts, and victims will see their online account balance increase rapidly as they "invest."

53. Initially, Victim-1 was able to make small withdrawals from Blockdcgchain. However, towards the middle of December, once Victim-1 appeared to have approximately $38 million on the platform, the account was "frozen," and Victim-1 could not withdraw funds.

54. Victim-1 was told by Blockdcgchain "customer service" that he was required to pay a

[3] The FBI believes that Victim-1 was initially using the publicly available app Strike, which describes itself as a "bitcoin app" allowing users to "buy bitcoin and send money globally," according to this LinkedIn company page: https://www.linkedin.com/company/strikebtc.

10% fee on the amount in the platform for "security" to make sure everything was done legitimately. After the amount was received, "customer service" stated that they would unfreeze the account and the risk margin (the 10%) would be refunded within 15 days.

55. It was at this point that Victim-1 became deeply suspicious that Blockdcgchain was a scam. The 10% fee that Blockdcgchain calculated was incorrect based on the amount in the account. "Customer service" also stated that a percentage was needed to pay taxes, and Victim-1 knew this was impossible because Blockdcgchain had no information about his total income and his potential tax liability

56. Throughout this process while Victim-1 was messaging with Blockdcgchain "customer service," Olivia was also placing pressure on Victim-1. She stated that she was out of money and was forced to take out another mortgage on her home. Olivia was consistently asking Victim-1 for money, and Victim-1 was stressed and overwhelmed.

57. Victim-1 attempted to take out another mortgage on a home he owned and even asked a friend for a loan. Fortunately, someone was renting the Victim-1's home, so Victim-1 was not able to obtain a second mortgage.

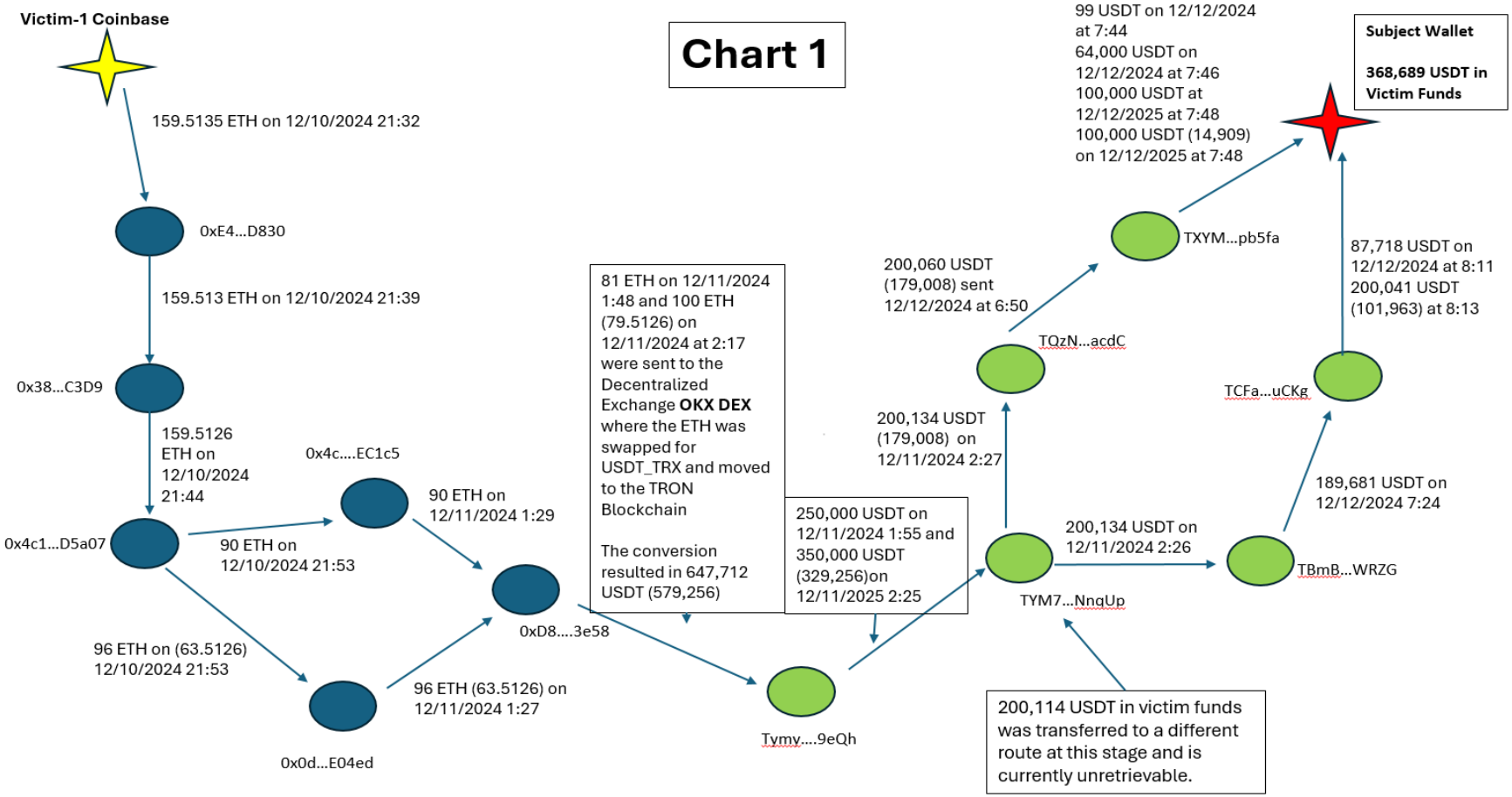
58. When Victim-1 contacted a friend for a loan, his friend and the friend's son started to look into Olivia. They discovered, through Google searches, that Olivia was using photos of the woman who was named "Miss Turkey" in 1995.

Blockchain Tracing of Victim-1's Funds

59. Blockchain tracing using a "Last-In-First-Out" principle was conducted on Victim-1's transactions with Blockdcgchain.

60. Chart 1 below shows the movement of Victim-1's funds from Coinbase into Blockdcgchain and then onwards. Chart 1 is followed by a detailed description of transactions.

In the chart below: (1) the yellow star represents Victim-1's initial Coinbase wallet; (2) the blue circles represent unhosted wallets on the Ethereum blockchain; (3) the green circles represented unhosted wallets on the Tron blockchain, and (4) the red star represents the **Subject Wallet Address.**



61. The FBI is aware from agents' prior cases that as CIF victims transfer their money onto the blockchain, victim funds are rapidly transferred out of the wallet into which they are deposited and transferred to other addresses controlled by the scammers.

62. Based on information provided by Victim-1, and records from the centralized cryptocurrency exchange Coinbase.com, Victim-1 made five withdrawals totaling 627.9436 ETH from his Coinbase.com account and sent these funds to a single unhosted wallet address.[4]

63. The funds located in the **Subject Wallet Address** stem from a transaction Victim-1 made on or about December 10, 2024, at 21:32 from his Coinbase account for 159.5135 Ethereum (ETH) to wallet 0xE46417988aD5d0A7f8644F9d24D7dc2A0117D830 (0xE46...D830).

64. On or about December 10, 2024 at 21:39, (0xE46...D830) sent 159.513 ETH to 0x38bBaEB044BbE777BCcEf5211098685040D1C3D9 (0x38..C3D9). On or about December 10, 2024 at 21:44, 0x38...C3D9 sent 159.5126 ETH to wallet address 0x4c12921Ffed713b8140b1E822db2a3fB139D5a07 (0x4c...5a07).

65. 0x4c...5a07 made two separate transactions, one to 0x4cC18C763376C37990D05ea4b695A648eEcEC1c5 (0x4c...C1c5) on or about December 10, 2024 at 21:53 for 90 ETH, and another to 0x0d1203c26821E6838b183aD604AE44ABecCE04ed (0x0d...04ed) on or about December 10, 2024 at 21:53 for 96 ETH, 63.5126 of which belonged to Victim-1.[5]

66. Both of these wallets sent these same amounts to 0xD852042CeE67D25Aa0ac8b663549EDA9F1a43e58 (0xD8...3e58) on or about December 11, 2024 at 1:29 and 1:27 respectively.

67. These transactions all had no discernible business purpose, and all of these transactions between addresses in this short time period resulted in small transaction fees being paid from the total amount from each transaction. I know from my training and experience that these are methods generally used by money launderers to obfuscate the nature, location, source, and ownership of their transactions.

[4] All times listed below are in UTC. All monetary values and times listed below are approximate.

[5] Using the Last-in-first-out (LIFO) method, the entire transaction making up the victim's funds is traced, but total victim funds are tracked separately as a part of said transaction.

68. 0xD8...3e58 made two transactions to a wallet address that a blockchain analytics tool labeled as a virtual currency exchange known as OKX DEX with Cluster ID 0x7D0CcAa3Fac1e5A943c5168b6CEd828691b46B36.

69. This exchange both transferred the transactions sent by 0xD8…3e58 from the Ethereum blockchain to the Tron blockchain, while also swapping the tokens from ETH to the stablecoin USDT.

70. The two Ethereum transactions were 81 ETH on or about December 11, 2024 at 1:48 and 100 ETH, 79.5126 of which belonged to Victim-1 Address TYmyBhSrWwj6iixHsE42jzZpUs3c9j9eQh (TYmy…9eQh) received 647,712 in converted USDT on the Tron blockchain, of which 579,256 belonged to Victim-1. *See* Chart 1 (center).

71. Money launderers will often "chain hop" (move cryptocurrency from one blockchain to a different blockchain) and exchange various cryptocurrencies for stablecoins to further obfuscate their transactions and frustrate law enforcement tracing efforts.

72. Money launderers are particularly drawn to USDT because of its low transactions fees and stability compared to other more volatile cryptocurrencies. USDT is compatible with 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.

73. On or about December 11, 2024, TYmy…9eQh made two transactions to TYM7CjpdCNaZEiyFkKzuzF3wYhA2HNnqUp (TYM7…nqUp) for 250,000 USDT at 1:55, and 350,000 USDT at 2:25. 329,256 USDT of the latter transaction belonged to Victim-1

74. At this point, the USDT was withdrawn from TYM7…nqUp in three transfers, in values of 200,114 and 200,134 USDT.

75. 200,114 USDT was transferred out of TYM7…nqUp to a different wallet address where Victim-1's assets were laundered in a manner which spread apart transfers into increasingly smaller values which were eventually deposited in a wide variety of cryptocurrency exchanges including some known to be uncooperative with U.S. law enforcement.

76. Victim-1's remaining funds were then split in two traceable tracks. TYM7…nqUp sent 200,134 USDT to TBmBhdcsybwXCu7mgYD3iZYk7g7EWDWRZG (TBmB...WRZG) on or about December 11, 2024, at 2:26.

77. TBmB...QRZG then sent 186,681 USDT to TCFaQfdJTgkN1WPCRhKAMr8uRwo8smuCKg (TCFa...uCKg) on or about December 12, 2024, at 7:24, after some of Victim-1's funds were sent to a different wallet.

78. Parallel to this, 200,134 USDT (179,008 of which belonged to Victim-1) was sent to TQzNB5WXHn6wZTwCdW6zFTcrmTyhVFacdC (TQzN...acdC) on or about December 11, 2024, at 2:27.

79. TQzN...acdC then sent 200,060 USDT (179,008 of which belonged to Victim-1) to TXYMDqcTsDq34gGx8czjZQPkapoKupb5fa (TXYM...b5fa) on or about December 12, 2024, at 6:50.

80. TXYM...b5fa then made four transfers on or about December 12, 2024, to the **Subject Wallet Address.** These transfers consisted of 99 USDT at 7:44, 64,000 USDT at 7:46, 100,000 USDT at 7:48, and 100,000 USDT (14,909 of which belonged to Victim-1) at 7:48.

81. Shortly after these transfers, TCFa...uCKg made two transfers on or about December 12, 2024 to the **Subject Wallet Address**. These transfers consisted of 87,718 USDT at 8:11 and 200,041 USDT at 8:13 (of which 101,963 USDT) belonged to Victim-1.

82. In total, these six transfers consolidated 368,689 USDT—that can be directly linked back to the fraud committed against Victim-1—at the **Subject Wallet Address**.

83. Based on experience, FBI agents believe that there was no legitimate financial purpose for why these addresses distributed and consolidated Victim-1's funds in a rapid series of transactions. Agents know from experience that moving victim funds in such a manner is how criminals regularly launder cryptocurrency on blockchains.

The Penultimate Wallets Through Which Victim-1's Funds Flowed Have Been Linked to Other CIF Investigations

84. Both wallets which directly transferred Victim-1's stolen funds into the **Subject Wallet Address** are linked to other CIF investigations as having fraud funds laundered through them.

85. The FBI traced 148,681 USDT stolen from another CIF victim, Victim-2, who lost $1,889,254 in a scam, to an account at the virtual currency exchange Poloniex.

86. Poloniex provided records showing all of Victim-2's traced funds were transferred from said Poloniex account to an address, which within one minute sent all of Victim-2's traced funds to TCFa...uCKg. The transfer of Victim-2's funds occurred in early October 2024, slightly two months prior to when Victim-1's funds were moved through TCFa...uCKg. As previously described, TCFa...uCKg also received cryptocurrency associated with Victim-1's funds, which it subsequently transferred to the **Subject Wallet Address**.

87. The FBI also traced Victim-2's funds into an account at the cryptocurrency exchange Bybit. Victim-2 had lost $250,000 in USDT and ETH from a CIF scam.

88. Bybit produced records showing that all of Victim-2's funds had been laundered through the Bybit exchange from the Ethereum blockchain and were subsequently converted to USDT and withdrawn on the Tron blockchain to address TXYM...pb5fa.

89. The transfer of Victim-2's funds occurred near the end of November 2024—less than a month before Victim-1's funds were moved through TXYM...pb5fa.

90. The Bybit user converted a total of 1,684,711 USDT from the Ethereum network and sent it to TXYM...pb5fa. The last transaction made by this user to TXYM...pb5fa occurred on or around December 15, 2024.

91. This final transaction was made only three days after Victim-1's funds were moved through TXYM...pb5fa.

92. FBI agents believe, based on the investigations, that the remainder of the Defendant Property at the **Subject Wallet Address** was obtained by defrauding other CIF victims. As previously described, TXYM...pb5fa also received funds related to the fraud perpetrated against Victim-1, which were subsequently sent to the **Subject Wallet Address.**

93. Based on these other victim complaints and the nature of how Victim-1's funds were moved in the blockchain tracing of Victim-1's funds described above, FBI agents believe that the wallets, including the **Subject Wallet Address**, make up a money laundering network.

94. The remainder of Victim-1's 627.9436 ETH lost to the fraud was dispersed across hundreds of unhosted wallets. Many of these unhosted wallets have direct and indirect relationships with one another, including the wallets Victim-1's funds passed through before they arrived at the **Subject Wallet Address**. Relationships in this context came in the form of directly sending and receiving cryptocurrency with one another, implying ongoing cooperation.

95. These relationships have no apparent business purpose aside from making it more difficult to trace the origin and destination of the funds that travel through them. The two prior wallets that were associated with two other FBI investigations, TCFa...uCKg and TXYM...pb5fa, also have direct connections and relationships to other wallets which received Victim-1's funds.

96. Both TCFa...uCKg and TXYM...pb5fa acted as consolidation wallets for scam proceeds that money launderers used to gather large amounts of cryptocurrency before dispersing these funds more broadly.

97. FBI agents believe that the funds moving through these accounts are involved in concealment money laundering because the transfers of funds depicted above have no apparent legitimate business purpose apart from disguising the nature, control, source, or ownership of the funds. The movement of funds between addresses incurs transaction fees that would be unnecessary in any legitimate, arms-length transaction involving cryptocurrency.

98. Based on agents' training and experience, they know that criminals will often conduct an otherwise unnecessary number of transactions in the transfer of funds to layer criminal proceeds and to conceal or disguise the nature, location, source, ownership, or control of those proceeds when they are ultimately transferred into a cryptocurrency exchange.

99. The number of transactions between wallets (or "hops") in quick succession involving Victim-1's funds is a strong indication that these transactions were performed in a manner meant to conceal or disguise the nature, location, source, ownership, or control of the proceeds of a specified unlawful activity, to wit, wire fraud and wire fraud conspiracy. This pattern of transfers also suggests that the money laundering activity was coordinated across addresses by the same money launderer, or group of launderers, in control of all the addresses.

100. Where the government shows that money launderer(s) commingled criminal proceeds with untraced funds in an account or address via transactions designed to conceal the nature, source, ownership, location, or control of criminal proceeds, then those commingled untraced funds are forfeitable as having facilitated—and therefore as having been "involved in"—money laundering. Accordingly, all of the funds in the **Subject Wallet Address** facilitated and were "involved in" the commission of concealment money laundering.

101. Additionally, based on agents' knowledge of how funds are generally laundered in CIF schemes, agents believe that multiple individuals have conspired to launder funds taken from victims of the schemes discussed in this affidavit, in violation of Section 1956(h) of Title 18, United States Code (conspiracy to commit money laundering).

Communications Regarding the Blocklisted Wallet Address

102. After Tether freezes an unhosted wallet address, the owner and/or others purporting to be the owners (claimants) may reach out to Tether to ask why Tether froze the address. Tether redirects those people to law enforcement. In this case, Tether redirected a potential claimant to the FBI email address cryptocurrencycomms@fbi.gov.

103. On February 26, 2025, the Tether Compliance team notified the FBI that someone named "Htebxprq9" with email htebxprz9@outlook.com claimed ownership of the **Subject Wallet Address**. An FBI agent responded to Htebxprq9 on March 27, 2025, and wrote the following:

> Hello, thank you for reaching out -
>
> Please use this email address for all communications going forward - (cryptocurrencycomms@fbi.gov).
>
> Please provide the following:
>
> - Proof of ownership of address TEZRLkhrWADL4LemEMHv25hnGK935GYzh4
> - Copy of your photo identification and a picture of yourself holding a piece of paper with the note "TEZRL....GYzh4" written on it
> - Your mailing address
> - Information about your current job and employer
> - An explanation for source of the USDT that was deposited into address TEZRLkhrWADL4LemEMHv25hnGK935GYzh4
> - List of all your other cryptocurrency addresses
>
> Happy to discuss all of the above in more detail if helpful.

Thank you very much and looking forward to discussing-[6]

104. The FBI did not receive a response from Htebxprq9.

105. On March 14, 2025, the Tether Compliance team notified the FBI that someone named "Lac Dalin" with email athasoudekerk@gmail.com claimed ownership of the **Subject Wallet Address.**

106. An FBI agent responded to Lac Dalin on March 27, 2025, and requested the same information that the FBI had sought from the first claimant.

107. The FBI did not receive a response.

108. On April 4, 2025, the Tether Compliance team notified the FBI that someone using the name "erwshn" with email address thasnihande@gmail.com claimed ownership of the **Subject Wallet Address**. An FBI agent responded to erwshn on April 4, 2025, and requested the same information that had been sought from the first two claimants.

109. The FBI did not receive a response.

110. Given that multiple purported claims were made to the FBI's email alias, but none of the claimants responded to the FBI's requests for additional information, agents believe that none of these claims was legitimate.

111. On May 21, 2025, a magistrate judge in the Northern District of California signed a seizure warrant for the Defendant Property

112. The seizure warrant was later executed by the government, and the Defendant Property was transferred to the custody of the U.S. Government.

COUNT ONE

Civil Forfeiture (Title 18, United States Code, Section 981(a)(1)(C)) for Wire Fraud (Title 18, United States Code, Section 1343)

113. Civil forfeiture of the proceeds of wire fraud is authorized by Title 18, United States Code, Section 981(a)(1)(C). Specifically, Section 981(a)(1)(C) authorizes forfeiture of "any property, real or personal, which constitutes or is derived from proceeds traceable to . . . any offense constituting

[6] In the actual email, this was a numbered list rather than a bulleted list.

'specified unlawful activity' (as defined in section 1956(c)(7) of this title), or a conspiracy to commit such offense." Section 1956(c)(7)(A) defines the term "specified unlawful activity" as including "any act or activity constituting an offense listed in section 1961(1) of this title." And Title 18, United States Code, Section 1961(1), in turn, includes violations of Title 18, United States Code, Section 1343 in its definition of racketeering activity.

114. The Defendant Property constitutes, and is derived from, the proceeds of wire fraud, and is thus subject to forfeiture pursuant to Title 18, United States Code, Section 981(a)(1)(C).

COUNT TWO

Civil Forfeiture (Title 18, United States Code, Section 981(a)(1)(A)) for Money Laundering (Title 18, United States Code, Section 1956(a)(1)(B)(i))

115. Civil forfeiture of property involved in a money laundering transaction, or property traceable to such property, is authorized by Title 18, United States Code, Section 981(a)(1)(A), which allows the United States to forfeit "any property, real or personal, involved in a transaction . . . in violation of section 1956 . . . of this title, or any property traceable to such property."

116. A violation of Title 18, United States Code, Section 1956(a)(1)(B)(i) occurs when a person conducts or attempts to conduct a financial transaction knowing that the transaction involves the proceeds of a specified unlawful activity when the transaction is designed in whole or part "to conceal or disguise the nature, the location, the source, the ownership or the control of the proceeds of the specified unlawful activity; or . . . to avoid a transaction reporting requirement under State or Federal law", or involves property "traceable to such property."

117. Wire fraud is a specified unlawful activity pursuant to Title 18, United States Code, Sections 1956(c)(7)(A) and 1961(1). Thus, the Defendant Property is subject to forfeiture pursuant to Title 18, United States Code, Section 981(a)(1)(A) because it was involved in, or is traceable to property involved in, money laundering transactions in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

\\

\\

PRAYER FOR RELIEF

118. The United States requests that due process issue to enforce the forfeiture of the above listed Defendant Property; that notice be given to all interested parties to appear and show cause why forfeiture should not be decreed; that the Court enter a judgment forfeiting the Defendant Property; and that the United States be awarded such other relief as may be proper and just.

DATED: November 10, 2025

Respectfully submitted,

CRAIG H. MISSAKIAN
United States Attorney

/s/
DANIEL PASTOR
Assistant United States Attorney

VERIFICATION

I, Christopher Calley, state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation (FBI). I am one of the agents working on this case. As such, I am familiar with the facts and the investigation leading to the filing of this Complaint for Forfeiture.

2. I have read the Complaint and affirm that the allegations contained therein are true.

* * *

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge. Executed this 10th day of November, 2025 in San Francisco, California.

*/s/*_____
Christopher Calley
Special Agent
Federal Bureau of Investigation