UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

Case No. 8:26-cv-

All USDT previously associated with following digital currency addresses on the Tron blockchain: TCZinsc8GhJR1K4VCpMCn8S1PDpJdpCSBT; and TQk9kucuy9fMKAWkcC4JJMK8yd7qSWyXvT,

Defendants.

VERIFIED COMPLAINT FOR FORFEITURE *IN REM*

The United States of America brings this complaint and alleges upon information and belief, in accordance with Rule G(2) of the Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions, as follows:

NATURE OF THE ACTION

1. This is a civil action *in rem* to forfeit to the United States, pursuant to 18 U.S.C. § 981(a)(1)(C) and 18 U.S.C. § 981(a)(1)(A), all USDT previously associated with the following addresses on the Tron blockchain:

   a. TCZinsc8GhJR1K4VCpMCn8S1PDpJdpCSBT (Defendant Address #1); and

   b. TQk9kucuy9fMKAWkcC4JJMK8yd7qSWyXvT (Defendant Address #2),

(collectively, the Defendant Assets).

2. The United States took custody of the Defendant Assets on or about August 12, 2025, pursuant to a Federal seizure warrant, after a finding of probable cause that the funds constituted proceeds of wire fraud offenses, in violation of 18 U.S.C. § 1343, and property involved in money laundering offenses, in violation of 18 U.S.C. § 1956(a)(1)(B)(i) (the Seizure Warrant). Thus, the Defendant Assets are subject to civil forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and (a)(1)(C).

3. The Defendant Assets are currently in the custody of the Internal Revenue Service – Criminal Investigation.

VENUE AND JURISDICTION

4. Venue properly lies in the Middle District of Florida pursuant to 28 U.S.C. § 1395(b), because pertinent acts giving rise to the forfeiture action occurred in the Middle District of Florida.

5. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1345, which provides the Court with jurisdiction over all civil actions commenced by the United States, and pursuant to 28 U.S.C. § 1355, which provides the Court with jurisdiction over actions to recover or enforce forfeitures.

6. This Court has *in rem* jurisdiction over the Defendant Assets because pertinent acts giving rise to the forfeiture occurred in the Middle District of Florida. 28 U.S.C. § 1355(b)(1)(A).

7. Because the Defendant Assets are in the government's possession, custody, and control, the United States requests that this Court issue an arrest warrant *in rem*, upon the filing of the complaint, pursuant to Supplemental Rule

G(3)(b)(i). Rule G(3)(b)(i) requires the Clerk to issue a warrant of arrest *in rem* for defendant property if such property is in the government's possession, custody, or control.

8. After the Court issues the warrant of arrest *in rem*, the United States will execute the warrant pursuant to 28 U.S.C. § 1355(d) and Supplemental Rule G(3)(c).

STATUTORY BASIS FOR FORFEITURE

9. The Defendant Assets represents proceeds of violations of 18 U.S.C. § 1343 (wire fraud) and are, therefore, subject to civil forfeiture by the United States, pursuant to 18 U.S.C. § 981(a)(1)(C). Section 981(a)(1)(C) provides for the civil forfeiture of any property, real or personal, which constitutes or is derived from proceeds from any offense constituting "specified unlawful activity" as defined in 18 U.S.C. § 1956(c)(7), or a conspiracy to commit such offenses. 18 U.S.C. § 981(a)(1)(C). Section 1956(c)(7)(A) incorporates the racketeering offenses under 18 U.S.C. § 1961. Wire fraud offenses in violation of 18 U.S.C. § 1343 are specified unlawful activities under 18 U.S.C. § 1961(1). *See* 28 U.S.C. § 981(a)(1)(C), 18 U.S.C. § 1956(c)(7)(A), and 18 U.S.C. § 1961(1).

10. Additionally, the Defendant Assets constitute property involved in transactions or attempted transactions in violation of 18 U.S.C. § 1956, or are traceable to such property and are, therefore, subject to civil forfeiture by the United States pursuant to 18 U.S.C. § 981(a)(1)(A). Section 981(a)(1)(A) provides for the civil forfeiture of any property, real or personal, involved in a transaction or

attempted transaction in violation of section 1956, or any property traceable to such property.

FACTS

11. Specific facts supporting the forfeiture of the Defendant Assets have been provided by Andrew Lorenz, Special Agent of the Internal Revenue Service – Criminal Investigation (IRS-CI), who states as follows.

12. Based on SA Lorenz's investigation, it appears that an individual in the Middle District of Florida was the victim of a cryptocurrency investment scam that began around August 2023 and continued through at least November 2023. After the victim was tricked into investing, the victim's funds were ultimately moved through layers of cryptocurrency addresses, without the victim's authorization, and into, in part, the Defendant Assets.

Background Related to Virtual Currency

13. **Virtual Currency (or Cryptocurrency):** Virtual currencies are digital tokens of value circulated over the internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank like traditional fiat currencies, such as the U.S. dollar, but rather are generated and controlled through computer software. Bitcoin (or BTC) and ether (ETH) are currently the most well-known virtual currencies in use. Other virtual currencies include USDT and TRX.

14. **Stablecoins:** Stablecoins are a type of virtual currency pegged to a commodity's price, such as gold, to a fiat currency, such as the U.S. dollar, or to a

different virtual currency. Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives. For example, USDC is a type of stablecoin pegged to the U.S. dollar.

15. **Tether (USDT):** Tether is a company that manages the smart contracts and the treasury (*i.e.,* the funds held in reserve) for USDT, a stablecoin pegged to the U.S. dollar. Other stablecoins backed by the United States dollar include USDC (discussed in the previous paragraph) and DAI.

16. **Swap:** A swap refers to the direct exchange of one cryptocurrency for another, without the need to first convert either currency into fiat money (like USD). A swap is essentially "buying" one crypto using another crypto directly, instead of buying with traditional currency. This process usually happens on a cryptocurrency exchange platform and is facilitated by smart contracts.

17. **Virtual Currency Address:** Virtual currency addresses are the particular virtual locations to or from which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of letters and numbers.

18. **Private Key:** Each virtual currency address is controlled through the use of a unique corresponding private key, a cryptographic equivalent of a password, which is needed to access the address. Only the holder(s) of an address's private key can authorize a transfer of virtual currency from that address to another address.

19. **Virtual Currency Wallet:** There are various types of virtual currency wallets, including software wallets, hardware wallets, and paper wallets. The virtual currency wallets at issue for the purposes of this affidavit are software wallets (i.e., a software application that interfaces with the virtual currency's specific blockchain and generates and stores a user's addresses and private keys). A virtual currency wallet allows users to store, send, and receive virtual currencies. A virtual currency wallet can hold many virtual currency addresses at the same time. Wallets hosted by third parties are often called "hosted wallets" because the third party retains a customer's funds until the customer is ready to transact with those funds. Conversely, wallets that allow users to exercise total, independent control over their funds are often called "unhosted" wallets.

20. **Blockchain:** The code behind many virtual currencies requires that all transactions involving that virtual currency be publicly recorded on what is known as a blockchain. The blockchain is essentially a distributed public ledger, run by a decentralized network of computers, containing an immutable and historical record of every transaction using that blockchain's technology. The blockchain can be updated multiple times per hour and records every virtual currency address that has ever received that virtual currency and maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies.

21. **Bridge:** A bridge refers to a technology that allows the transfer of cryptocurrency assets between different blockchain networks, essentially acting as a

connection point to move tokens from one chain to another, enabling interoperability between various blockchain ecosystems.

22. **Blockchain Explorer:** These explorers are online tools that operate as a blockchain search engine allowing users the ability to search for and review transactional data for any addresses on a particular blockchain. A blockchain explorer is software that uses API and blockchain nodes to draw data from a blockchain and uses a database to arrange and present the data to a user in a searchable format.

23. **Virtual Currency Exchanges (VCEs):** VCEs are trading and/or storage platforms for virtual currencies, such as BTC and ETH. Many VCEs also store their customers' virtual currency in virtual currency wallets. As stated above, these wallets can hold multiple virtual currency addresses associated with a user on a VCE's network. Because VCEs act as money services businesses, they are legally required to conduct due diligence of their customers, including Know Your Customer (or KYC) checks, and to have anti-money laundering programs in place (if they operate and service customers in the United States). 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).

24. **Blockchain Analysis:** It is virtually impossible to look at a sole transaction on a blockchain and immediately determine the identity of the individual

behind said transaction. That is because blockchain data generally only consists of alphanumeric strings and timestamps. That said, law enforcement can obtain leads regarding the identity of the owner of an address by analyzing blockchain data to figure out whether that same individual is connected to other relevant addresses on the blockchain. To do so, law enforcement can use blockchain explorers, as well as commercial services offered by several different blockchain-analysis companies. These companies analyze virtual currency blockchains and attempt to identify the individuals or groups involved in transactions. "For example, when an organization creates multiple [BTC] addresses, it will often combine its [BTC] addresses into a separate, central [BTC] address (i.e., a 'cluster'). It is possible to identify a 'cluster' of [BTC] addresses held by one organization by analyzing the [BTC] blockchain's transaction history. Open-source tools and private software products can be used to analyze a transaction." *United States v. Gratkowski*, 964 F.3d 307, 309 (5th Cir. 2020). Through numerous unrelated investigations, law enforcement has found the information provided by these tools to be reliable.

Background

25. On or about December 20, 2023, the Victim, a 58-year-old resident of Tampa, Florida, was interviewed by IRS-CI after he contacted law enforcement regarding a cryptocurrency investment scam.

26. According to the Victim, on or about August 21, 2023, he was contacted on WeChat, a Chinese social media application, by an individual with the English name of Lindsay Luo and Chinese name of Ya-li Luo (Luo). Luo told the

Victim that she was from the same city in China as the Victim and that she currently lives in Portland, Oregon. Luo and the Victim began communicating over WeChat, a Chinese messaging service that enables users to chat directly or in groups using text, voice, and video. After about one or two weeks, Luo started talking to the Victim about investments. Luo initially suggested that the Victim invest in the Philadelphia Gold and Silver Index (XAU). Luo showed the Victim a demo of a trading website for about two or three days.

27. According to the Victim, Luo then showed the Victim her live trading website, Dgctcfx.com (Dgctcfx). The website purported to show that Luo's investments were making a lot of money. The Victim agreed to invest with Luo through Dgctcfx. Luo instructed the Victim to wire money to two banks located in Hong Kong. Luo, or a customer service representative on the Dgctcfx website, provided him wiring instructions. Luo also gave the Victim wiring instructions via phone conversations. According to records provided by the Victim, in September and October 2023, the Victim sent three wires totaling approximately $598,799 from his personal bank accounts to the Hong Kong banks. After these wires, the Victim was able to see what he thought were his investments on the Dgctcfx platform.

28. The Victim informed that he was also instructed to open a separate VCE account (VCE 1) and deposit money into this account. The Victim thinks that Luo setup his VCE 1 account and provided him two factor authentication for the account via a Google QR code. Luo showed him how to buy cryptocurrency and transfer money between different cryptocurrency coins.

29. The Victim stated that, later, Luo contacted the Victim on Telegram, an encrypted social media and messaging platform, and instructed the Victim to make transfers on VCE 1 in cryptocurrency. Luo instructed the Victim to send money from VCE 1 to a cryptocurrency address that Luo told him was ultimately going to Dgctcfx to be invested.

30. The Victim stated that Luo repeatedly told the Victim to invest more money through VCE 1 and told him about promotions that enticed the Victim to invest more. Records provided by the Victim show that he deposited a total of approximately $2,744,142 at VCE 1, which was later sent to a cryptocurrency address provided by Luo. Luo told him when to buy and sell various cryptocurrencies. The Victim was fraudulently led to believe that his trading gains on Dgctcfx totaled approximately $1,137,999. Instead, and as will be detailed below, the Victim's funds were ultimately moved from VCE 1, through layers of cryptocurrency addresses, and on, in part, to the Defendant Assets.

31. The Victim stated that the last time that the Victim sent money or contacted Luo was on or about November 7, 2023, which was when the Victim realized Dgctcfx was a scam website. The Victim tried to withdraw money from Dgctcfx but was told that he would have to pay a tax to get his money out. The Victim has not been able to retrieve any of the funds that were wired to Hong Kong banks or sent via VCE 1, which, together, totaled approximately $3,339,794.

32. SA Lorenz has reviewed records provided by the Victim including messages between the Victim and Lou, emails between the Victim and Dgctcfx,

screenshots of the Dgctcfx website, and the Victim's bank and VCE 1 statements, all of which corroborated the information provided by Victim.

Analysis of VCE 1 Records

33. The Victim provided IRS-CI his VCE 1 account number (Victim Account). As part of our investigation, IRS-CI obtained records from VCE 1 regarding the Victim Account.

34. The Victim Account was opened on September 5, 2023, and is held in the name of the Victim. On October 3, 2023, 100 USDT and 3.55 Ether (ETH) were transferred to the Victim Account.[1] The Victim told IRS-CI that he believes that Luo initiated these transactions. Based on his investigation, SA Lorenz believes these may have been test transfers to confirm that the Victim Account had been established correctly.

35. Between October 3, 2023, and November 6, 2023, the Victim deposited a total of approximately $2,744,142 into the Victim Account. Between October 4, 2023, and November 7, 2023, most of these funds were then converted to cryptocurrency ETH, Ethereum Classic (ETC), and Decentral Games Governance (xDG).[2] Once converted, the cryptocurrency stayed in the Victim Account until the funds were transferred to address 0xde56f743eb574c697f4064693c4ad66ab05e2301 (Address A) on the Ethereum blockchain.

[1] All dates and figures are approximate figures based on records and data obtained from VCE 1 and blockchain analysis tools.

[2] Approximately $40,469 in fees were paid to convert the funds to cryptocurrency.

36. According to the VCE, the Victim Account was closed on or about December 21, 2023. At or around the time of closing, approximately $16,963.27 in remaining funds were returned to the Victim.

Blockchain Analysis and Tracing of Funds into the Defendant Assets

37. As detailed above, after the Victim Account was established, the Victim's funds were initially moved out of the account to Address A, which appears to have been used as an initial layer in a complicated laundering process. The funds were then moved through numerous other cryptocurrency addresses, swapped for other coins, bridged to a different blockchain, and moved, at least in part, to the Defendant Assets. Diagrams illustrating the movement of the Victim's funds through the blockchain and into the Defendant Assets are attached as Exhibits 1, 2, and 3, and the tracing is detailed below.

A. Exhibit 1: Movement of Victim Funds from Address A to Address D

38. Between October 7, 2023, and October 20, 2023, there were three transfers from the Victim Account to Address A, totaling approximately 1,050.74 ETH (equivalent to approximately $1,702,938). On or about October 27, 2023, a total of approximately 1,050.74 ETH (equivalent to approximately $1,895,705) was then transferred from Address A to 0x36f73ff1bb343446b0bd0042f413028ff3e9347b (Address B1) in three separate transactions. Within less than 30 minutes, the ETH in Address B1 (equivalent to approximately $1,897,000 USDT) was swapped to USDT using Tokenlon, a VCE on the Ethereum blockchain that provides coin swap services, commingled with other funds and transferred – a total of 2,482,813 USDT

(equivalent to approximately $2,480,546) -- to address 0xf04ccbcbb6a5b749c031e5e5bc63e0256bd81ba1 (Address B2).

39. On November 24, 2023, and November 29, 2023, 1,765,902 USDT (equivalent to approximately $1,776,220) and 716,908 USDT (equivalent to approximately $713,987), respectively, were transferred from Address B2 to 0x9f30654d708a2fd0c28855f8a5ee34a0ce0b587c (Address D).

40. There was also an additional transfer of the Victim's funds from the Victim Account to Address A in November that followed a different path, but those funds were also ultimately sent to Address D. Specifically, on November 7, 2023, 544.12 ETH (approximately $1,038,057.00) was transferred from the Victim Account to Address A. Three days later, these funds -- approximately 544.31 ETH (equivalent to approximately $1,162,710) – were transferred from Address A to 0x920cc7b0a1d758c30955e563e102e2ddeb34cb0e (Address C1). Less than 15 minutes later, the 544.31 ETH in Address C1 (equivalent to approximately 1,163,000 USDT) was swapped to USDT using Tokenlon and transferred -- approximately 1,125,236 USDT (equivalent to approximately $1,124,928) -- from Address C1 to 0xc1e8b758fefca645e096f4004c0d6bbf63a3a1f0 (Address C2). The next day, these funds (1,125,236 USDT) were then transferred from Address C2 to 0x25632ae4fedd4121d81fe2d0956c2484f0c5502c (Address C3). Lastly, on November 24, 2023, the funds in Address C3 were commingled with other funds and approximately 1,980,760 USDT (equivalent to approximately $1,992,334) was transferred from Address C3 to Address D.

41. In total, between October 7, 2023, and November 29, 2023, Victim funds totaling approximately $2,740,995 were moved from the Victim Account, through layers of addresses, commingled with other funds, and on, at least in part, to Address D. The rapid movement of the Victim funds through multiple layers of cryptocurrency addresses as detailed above serves no purpose other than to conceal the source, origin, nature and ownership of these criminal proceeds.

B. Exhibit 2: Movement of Victim Funds from Address D to Bridgers

42. The USDT that was transferred to Address D on November 24, 2023, approximately 3,746,662 USDT (equivalent to approximately $3,768,554), was swapped on the same day to DAI, a stable coin, using 1inch Network, a VCE that provides coin swapping services. Also, that same day, (1) 785,658 DAI (equivalent to approximately $790,675) was transferred from Address D to 0x71868cb168fabecbd4d6ee4dfa8af2f2fa67beae (Address E1); (2) 1,773,350 DAI (equivalent to approximately $1,784,673) was transferred from Address D to 0x5da61f0b2318b5af7a2926beb12349beeb882098 (Address F1); and (3) 956,585 DAI (equivalent to approximately $962,693) was transferred from Address D to 0x87bf3efdee30824ccc9e702e735a048064ceee21 (Address G1). On January 17, 2024, approximately 1,773,350 DAI in Address F1 was transferred to 0xfe9fe2ef61faf6e291b06903dff85df25a989498 (Address F2). Further, on January 25, 2024, the approximately 785,658 DAI in Address E1 was transferred to 0x59b95a54045002e7eb7558930b71bb4606ae8cba (Address E2) and the

approximately 956,585 DAI in Address G1 was transferred to 0x8ff148cddb375f0ca35cd86e0add59a4a855dff0 (Address G2).

43. The DAI in Addresses F2 and E2 remained in these addresses for several months. However, on December 13, 2024, 1,535,665 DAI (equivalent to approximately $1,545,107) was transferred from Address F2 to 0xafde38c6fe29d0deac6f4404ca9fbe6f75d882e8 (Address F3) and then swapped for USDT using OKX, a Chinese based VCE. The same day, approximately 867,879 USDT (equivalent to approximately $862,315) was transferred to 0xfd6ead5eab787df0decf409f6b088312e7b38e6b (Address H) via two separate transfers and then bridged from the Ethereum blockchain to the Tron blockchain using a cross-chain service called Bridgers.

44. On December 15, 2024, and December 16, 2024, an additional 72,001 USDT (equivalent to approximately $71,673) and 364,793 USDT (equivalent to approximately $366,216) were transferred from Address F3 to Address H and then bridged to the Tron blockchain using Bridgers.

45. On February 13, 2025, the funds connected to the Victim that had been transferred to Address E2 on January 25, 2024 (*see* ¶ 42, above) were commingled with other funds and then 3,380,433 DAI (equivalent to approximately $3,357,780) was transferred from Address E2 to 0xe0c55c4c01bd05e1014858c16f273587ce823774 (Address E3). After that, approximately 982,373 DAI was swapped for USDT using Wintermute, a Singapore based VCE. The same day, approximately 988,030 USDT (equivalent to approximately $994,338) was transferred to Address H via two

separate transfers and then bridged from the Ethereum blockchain to the Tron blockchain using Bridgers.

46. In total, between December 2024 and February 2025, approximately 2,292,702 USDT was transferred to Bridgers through transactions containing the Victim's funds.

C. Exhibit 3: Movement of Funds from Bridgers to Defendant Assets

47. From Bridgers, the funds were ultimately moved through a series of rapid transfers to the Defendant Assets. First, on December 13, 2024, there were two transfers from Bridgers, totaling approximately 865,271 USDT (equivalent to approximately $865,406), to TU1VZFVqUhn3uCN3AoJvxXxyzxEQ7ytUg4 (Layering Address # 1). Less than an hour later, the equivalent amount of USDT (865,271 USDT) was then transferred from Layering Address # 1 to Defendant Address # 1. Approximately three minutes after that, 500,000 USDT (equivalent to approximately $500,078) was then transferred from Defendant Address # 1 on to another address and commingled with other funds from unknown sources. Approximately three minutes later, there were two more transfers on from this address of approximately 300,000 USDT, each, that were sent to two separate addresses. The rapid movement of these funds through layers of addresses served no legitimate purposes and was designed to conceal and disguise the nature, location, source, control or ownership of the criminal proceeds. Tether placed an internal freeze on the funds held in Defendant Address # 1 on December 16, 2024, based on suspicions of its connection to fraud and money laundering.

48. Further, on February 13, 2025, approximately 487,661 USDT (equivalent to approximately $487,704) was transferred from Bridgers to TYi7yhjqZjRY9HoyxSoWrHLzdRHzWUTnSS (Layering Address #2) and then to Defendant Address # 2. Less than an hour later, approximately 497,401 USDT (equivalent to approximately $497,446) was transferred from Bridgers to Layering Address # 2, commingled with funds from an unknown source, and approximately 698,340 USDT (equivalent to approximately $698,402) was then transferred from Layering Address # 2 to Defendant Address # 2. Tether placed an internal freeze on the funds held in Defendant Address # 2 on February 18, 2025, based on suspicions of its connection to fraud and money laundering.

D. Summary of Defendant Assets

49. As detailed above, there is probable cause to believe that the Defendant Assets received transfers involving the Victim's funds. The Defendant Assets also facilitated the laundering of these fraudulent proceeds by serving as unnecessary, additional layers in the movement of these funds. The rapid movement of the Victim's funds through multiple layers of cryptocurrency addresses, and the commingling of the fraudulent proceeds with funds from other, unknown sources before their deposit, in part, into these anonymous, unhosted virtual currency addresses, served no legitimate purpose other than to conceal and disguise the nature, location, source, control or ownership of the criminal proceeds.

50. Below is a summary of the typical transaction pattern and volume within each of the Defendant Assets, a recap of their connection to the Victim's funds, and the amount seized.

a. **Defendant Address # 1:** Defendant Address # 1 was first active on July 31, 2024. Between July 31, 2024, and January 20, 2025, cryptocurrency transferred into Subject Address # 2 (approximately 657 incoming transactions) totaled approximately $5,953,657, while outgoing transactions (approximately 18) totaled approximately $4,959,861. Based on this, it appears that Defendant Address # 1 was primarily used to receive and move funds on to other addresses. With regards to the Victim's funds, as detailed above, on December 13, 2024, Defendant Address # 1 received approximately 865,271 USDT connected to the Victim from Layering Address # 1 and transferred 500,000 USDT on to an additional layering address that same day. *See* Exhibit 3. On December 16, 2024, Tether placed an internal freeze on Defendant Address # 1, which prohibited any further outgoing transactions, based on suspicions of its connection to fraud and money laundering. On August 12, 2025, pursuant to the Seizure Warrant, Tether transferred a total of 995,357.62 USDT traceable to Defendant Address # 1 to a wallet controlled by the United States. Based on the foregoing, including the volume of transactions, the transactions connected to our Victim, and the use of the address to receive funds and rapidly move them on, there is probable cause to believe that the funds seized from Defendant Address # 1 constitute proceeds traceable to wire fraud offenses and

property involved in, or traceable to, transactions designed to conceal the true nature, source, ownership, and/or control of the wire fraud proceeds.

b. **Defendant Address # 2:** Defendant Address # 2 was first active on January 25, 2025, and appears to be a new address that was established to launder funds after other layering addresses, including Layering Address # 1 and Defendant Address # 1, were frozen by Tether. As detailed above, on February 13, 2025, Defendant Address # 2 received approximately 1,186,000 USDT connected to the Victim from Layering Address # 2. *See* Exhibit 3. On February 18, 2025, Tether placed an internal freeze on Defendant Address # 2, which prohibited any further outgoing transactions, based on suspicions of its connection to fraud and money laundering. On August 12, 2025, pursuant to the Seizure Warrant, Tether transferred a total of 1,759,238.00 USDT traceable to Defendant Address # 2 to a wallet controlled by the United States. Based on the foregoing, including the transactions connected to our Victim, there is probable cause to believe that all funds seized from Defendant Address # 2 are proceeds traceable to wire fraud offenses and constitute property involved in, or traceable to, transactions designed to conceal the true nature, source, ownership, and/or control of the wire fraud proceeds.

51. As required by Supplemental Rule G(2)(f), the facts set forth herein support a reasonable belief that the government will be able to meet its burden of proof at trial. Specifically, they support a reasonable belief that the government will be able to show by a preponderance of the evidence that the Defendant Assets are

derived from proceeds of wire fraud, and also constitute property involved in, or traceable to, money laundering violations.

CONCLUSION

WHEREFORE, pursuant to Supplemental Rule G, Plaintiff United States of America requests that this Court initiate a process of forfeiture against the Defendant Assets, and duly notice all interested parties to appear and show cause why the forfeiture should not be decreed. The United States further requests the Court order the Defendant Assets forfeited to the United States for disposition according to law and grant the United States such other and further relief as this case may require.

Dated: January 8th, 2026

Respectfully submitted,

GREGORY W. KEHOE
United States Attorney

By: _____

Suzanne C. Nebesky
Assistant United States Attorney
Florida Bar No. 59377
400 N. Tampa Street, Suite 3200
Tampa, Florida 33602
Telephone: (813) 274-6000
Facsimile: (813) 274-6220
E-mail: suzanne.nebesky@usdoj.gov

VERIFICATION

Pursuant to 28 U.S.C. § 1746, I, Andrew Lorenz, declare under penalty of perjury that:

I am a Special Agent with the Internal Revenue Service – Criminal Investigation. I have read the foregoing Verified Complaint for Forfeiture *in Rem* and have personal knowledge that the matters alleged as fact in the Complaint are true.

I have acquired my knowledge in this matter through my personal experience, observation, investigation, and training, and from witnesses, records, and other law enforcement officers.

Executed this 7th day of January, 2026.

Andrew Lorenz, Special Agent
Internal Revenue Service – Criminal Investigation