IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF OHIO

EASTERN DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. 4,340,000 TETHER ("USDT") CRYPTOCURRENCY, VALUED AT APPROXIMATELY $4,340,000, FORMERLY ASSOCIATED WITH CRYPTOCURRENCY ADDRESS BEGINNING/ENDING 0xa17 . . . 44f0021, 3,290,000 TETHER ("USDT") CRYPTOCURRENCY, VALUED AT APPROXIMATELY $3,290,000, FORMERLY ASSOCIATED WITH CRYPTOCURRENCY ADDRESS BEGINNING/ENDING 0x4e5 . . . d47abb5, and 577,578 TETHER ("USDT") CRYPTOCURRENCY, VALUED AT APPROXIMATELY $577,578, FORMERLY ASSOCIATED WITH CRYPTOCURRENCY ADDRESS BEGINNING/ENDING 0xafd . . . b2378a5, Defendants.	)	CASE NO. JUDGE **COMPLAINT IN FORFEITURE**

NOW COMES plaintiff, the United States of America, by its attorneys, Carol M. Skutnik, Acting United States Attorney for the Northern District of Ohio, and James L. Morford, Assistant United States Attorney, and files this Complaint in Forfeiture, respectfully alleging on information and belief as follows in accordance with Supplemental Rule G(2) of the Federal Rules of Civil Procedure:

I. *JURISDICTION AND INTRODUCTION.*

1. This Court has subject matter jurisdiction over an action commenced by the United States under 28 U.S.C. Section 1345, and over an action for forfeiture under 28 U.S.C. Section 1355(a). This Court also has jurisdiction over this particular action under 18 U.S.C. Section 981(a)(1)(C) (civil forfeiture authority: wire fraud/conspiracy) and 18 U.S.C. Section 981(a)(1)(A) (civil forfeiture authority: money laundering).

2. This Court has *in rem* jurisdiction over the defendant properties pursuant to: (i) 28 U.S.C. Section 1355(b)(1)(A) because acts giving rise to the forfeiture occurred in this district; and, (ii) 28 U.S.C. Section 1355(b)(1)(B), incorporating 28 U.S.C. Section 1395, because the action accrued in this district.

3. The defendant properties are presently in the custody of the United States Marshals Service (USMS). This Court will have control over the defendant properties through service of arrest warrant(s) *in rem*, which the USMS will execute upon the defendant properties. *See*, Supplemental Rules G(3)(b) and G(3)(c).

4. Venue is proper in this district pursuant to: (i) 28 U.S.C. Section 1355(b)(1)(A) because acts giving rise to the forfeiture occurred in this district; and, (ii) 28 U.S.C. Section 1395 because the action accrued in this district.

5. The defendant properties are subject to forfeiture to the United States under 18 U.S.C. Section 981(a)(1)(C) as property which constitutes, or is derived from, proceeds traceable to an offense(s) constituting "specified unlawful activity" (SUA) - as defined in 18 U.S.C. Section 1956(c)(7), with reference to 18 U.S.C. Section 1961(l) - namely: wire fraud, in violation of 18 U.S.C. Section 1343, and conspiracy to commit wire fraud, in violation of 18 U.S.C. Section 371.

6. The defendant properties also are subject to forfeiture to the United States under 18 U.S.C. Section 981(a)(1)(A) as property that was involved in a transaction(s) - or attempted transaction(s) - in violation of 18 U.S.C. Section 1956(a)(1)(B)(i) (sometimes referred to as concealment money laundering), 18 U.S.C. Section 1957 (sometimes referred to as transactional money laundering), and/or 18 U.S.C. Section 1956(h) (money laundering conspiracy), or as property traceable to such property.

II. *DESCRIPTION OF THE DEFENDANT PROPERTIES.*

7. The following properties are the defendant properties in the instant case:

a.) 4,340,000 Tether ("USDT") cryptocurrency, valued at approximately $4,340,000, formerly associated with the cryptocurrency address beginning/ending 0xa17 . . . 44f0021 on the Ethereum blockchain. On or about June 21, 2024, the USDT tokens at the cryptocurrency address were frozen by Tether Limited Inc. ("Tether Limited"). Thereafter, pursuant to a federal seizure warrant issued by U.S. Magistrate Judge Jonathan D. Greenberg on August 21, 2024, Tether Limited "burned" the USDT tokens associated with the cryptocurrency address and, on or about November 20, 2024, reissued the equivalent amount of USDT tokens [namely, 4,340,000 USDT] to a U.S. law enforcement-controlled virtual currency wallet. The cryptocurrency address beginning/ending 0xa17 . . . 44f0021 is referred to in the following paragraphs as "**ADDRESS A-7**."

b.) 3,290,000 Tether ("USDT") cryptocurrency, valued at approximately $3,290,000, formerly associated with the cryptocurrency address beginning/ending 0x4e5 . . . d47abb5 on the Ethereum blockchain. On or about June 25, 2024, the USDT tokens at the cryptocurrency address were frozen by Tether Limited Inc. ("Tether Limited"). Thereafter, pursuant to a federal seizure warrant issued by U.S. Magistrate Judge Jonathan D. Greenberg on August 21, 2024,

Tether Limited "burned" the USDT tokens associated with the cryptocurrency address and, on or about November 20, 2024, reissued the equivalent amount of USDT tokens [namely, 3,290,000 USDT] to a U.S. law enforcement-controlled virtual currency wallet. The cryptocurrency address beginning/ending 0x4e5 . . . d47abb5 is referred to in the following paragraphs as "**ADDRESS A-8**."

c.) 577,578 Tether ("USDT") cryptocurrency, valued at approximately $577,578, formerly associated with the cryptocurrency address beginning/ending 0xafd . . . b2378a5 on the Ethereum blockchain. On or about June 21, 2024, the USDT tokens at the cryptocurrency address were frozen by Tether Limited Inc. ("Tether Limited"). Thereafter, pursuant to a federal seizure warrant issued by U.S. Magistrate Judge Jonathan D. Greenberg on August 21, 2024, Tether Limited "burned" the USDT tokens associated with the cryptocurrency address and, on or about November 20, 2024, reissued the equivalent amount of USDT tokens [namely, 577,578 USDT] to a U.S. law enforcement-controlled virtual currency wallet. The cryptocurrency address beginning/ending 0xafd . . . b2378a5 is referred to in the following paragraphs as "**ADDRESS A-9**."

III. *STATUTES.*

8. *Offense Statutes*. This Complaint in Forfeiture relates to violations of 18 U.S.C. Section 1343 (wire fraud), 18 U.S.C. Sections 1956 and 1957 (money laundering), and conspiracy to commit such offenses, in violation of 18 U.S.C. Section 371 and 18 U.S.C. Section 1956(h).

9. *Wire Fraud*: 18 U.S.C. Section 1343 makes it a crime for anyone, 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, to transmit or cause to be

transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice.

10. *Money Laundering [§ 1956(a)(1)(B)(i)]*: 18 U.S.C. Section 1956(a)(1)(B)(i) makes it a crime to conduct or attempt to conduct "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."

11. *Money Laundering [§ 1957]*: 18 U.S.C. Section 1957 prohibits an individual from engaging or attempting to engage "in a monetary transaction in criminally derived property of a value greater than $10,000.00 and derived from specified unlawful activity."

12. *Money Laundering [§ 1956(h)]*: 18 U.S.C. Section 1956(h) provides that "[a]ny person who conspires to commit any offense defined in this section or section 1957 shall be subject to the same penalties as those prescribed for the offense the commission of which was the object of the conspiracy."

13. *Forfeiture Statutes*:

a.) *Wire Fraud*: Under 18 U.S.C. Section 981(a)(1)(C), any property - real or personal - which constitutes or is derived from proceeds traceable to a violation of 18 U.S.C. Section 1343 (wire fraud), or a conspiracy to commit such offense, is subject to forfeiture.

b.) *Money Laundering*: Under 18 U.S.C. Section 981(a)(1)(A), any property - real or personal - "involved in" or traceable to an offense in violation of 18 U.S.C. Section 1956(a)(1)(B)(i) (concealment money laundering), 18 U.S.C. Section 1957 (transactional money

laundering), and/or 18 U.S.C. Section 1956(h) (money laundering conspiracy) is subject to forfeiture.

14. Particularly, under a money laundering theory of forfeiture, the government is not limited to forfeiting only the criminal proceeds involved in the money laundering transaction. Rather, the government may also forfeit "other funds" involved in the money laundering transaction where those funds were part of the corpus of the laundering transaction or where those "other funds" facilitated the money laundering transaction.

15. *"Corpus" of the Laundering Transaction*: Where the financial transaction is a transfer of a commingled sum of money from cryptocurrency address A to address B, if that transaction constituted a money laundering transaction, then the entire sum transferred is forfeitable as the corpus of the money laundering offense. The SUA proceeds involved in the financial transaction - as well as any "other funds" transferred with it - constitute the corpus of the money laundering transaction; both are subject to forfeiture.

16. *Facilitation of a Laundering Transaction*: "Other funds" that facilitate the money laundering conduct - by helping conceal the nature, source, ownership, or control of the cryptocurrency traceable to a fraud victim - are likewise subject to forfeiture. For example, "other funds" in a cryptocurrency address into which SUA proceeds are transferred as part of a concealment money laundering offense - along with any "other funds" transferred with the SUA proceeds as part of the concealment money laundering offense - are subject to forfeiture as property "involved in" the offense. In both instances, the "other funds" commingled with the SUA proceeds obfuscate the origin or existence of the SUA proceeds.

17. *Money Laundering Conspiracy*: In a conspiracy case, all properties involved in the course of conduct constituting the money laundering conspiracy - including "untainted property" - are subject to forfeiture.

IV. *BACKGROUND ON CRYPTOCURRENCY.*

18. *Virtual Currency*: Virtual currencies are digital tokens of value circulated over the Internet. Virtual currencies are typically 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. Different virtual currencies operate on different blockchains, and there are many different, widely used virtual currencies currently in circulation. Bitcoin (or BTC) and Ether (ETH) are currently the most well-known virtual currencies in use. BTC exists on the BTC blockchain and ETH exists on the Ethereum network.

19. *Tether*: Tether (USDT) is a "stablecoin," a type of blockchain-based currency that is tied - or tethered - to a fiat currency. USDT exists on several third-party blockchains, including Ethereum. USDT is a centralized stablecoin, which means the cryptocurrency is backed by U.S. Dollars and other assets held by Tether Limited. Tether Limited is a company that manages the smart contracts and the treasury (*i.e.*, the funds held in reserve) for USDT tokens. Tether seeks to peg USDT to the U.S. dollar at a 1:1 ratio.

20. *Virtual Currency Address*: Virtual currency addresses are the specific virtual locations to 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.

21. *Private Key*: Each virtual currency address is controlled using 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' private key can authorize a transfer of virtual currency from that address to another address.

22. *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 in the instant case 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.

23. *Hosted Wallets:* Wallets that are hosted by third parties are referred to as "hosted wallets" because the third party retains a customer's funds until the customer is ready to transact with those funds.

24. *Virtual Currency Exchanges (VCEs)*: VCEs are trading and/or storage platforms for virtual currencies. Many VCEs also store their customers' virtual currency in virtual currency wallets. Because VCEs act as money services businesses, they are legally required to conduct due diligence of their customers (*i.e.*, Know Your Customer - "KYC" - checks) and to have anti-money laundering programs in place to the extent they operate and service customers in the United States.

25. *Unhosted Wallets*: An "unhosted wallet", also known as cold storage or self-custody, is a cryptocurrency wallet that is not hosted or controlled by a cryptocurrency exchange. Unhosted wallets allow users to exercise total, independent control over their funds.

26. *Blockchain*: Many virtual currencies publicly record all of their transactions on what is known as a blockchain. The blockchain is essentially a distributed public ledger, run by the decentralized network of computers, containing an immutable and historical record of every

transaction utilizing that blockchain's technology. The blockchain can be updated multiple times per hour; it records every virtual currency address that has ever received 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.

27. *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 address 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.

28. API stands for application programming interface, which is a set of definitions and protocols for building and integrating application software.

29. For all cryptocurrency transactions detailed herein, dates, times, amounts, and valuations are all approximations.

V. *BACKGROUND OF INVESTIGATION.*

30. The FBI Cleveland Field Office is investigating cryptocurrency confidence fraud scams perpetrated on victims throughout the United States, including in the Northern District of Ohio.

31. The fraud scheme detailed below is a particular type of investment fraud scheme and is known by an unsavory term - not repeated here - derived from the foreign-language word used to describe the scheme.

32. Based on data submitted to the FBI's Internet Crime Complaint Center in 2022, the particular type of investment fraud scheme detailed below targeted tens of thousands of victims in the United States and resulted in the loss of over two billion dollars in private assets.

The scheme begins by fraudsters contacting potential victims through seemingly misdirected text messages, dating applications, or professional meet-up groups. Next, using various means of manipulation, the fraudster gains the victim's affection and trust.

33. Once trust is established, the fraudster recommends cryptocurrency investment by touting their own success, or that of an associate. Means of carrying out the scheme vary, but a common tactic is to direct a victim to a fake "investment platform" hosted on a website.

34. These websites, and the "investment platforms" hosted there, are created by fraudsters to appear to be legitimate platforms. The fraudster assists the victim with opening a cryptocurrency account, often on a U.S.-based virtual currency exchange (VCE) such as Crypto.com, and then walks the victim through transferring money from a bank account to that cryptocurrency account. Next, the victim will receive instructions on how to transfer their cryptocurrency assets to the fake investment platform.

35. On its surface, the platform shows lucrative returns, encouraging further investment; underneath, all transferred funds are routed to a cryptocurrency wallet address controlled completely by the fraudsters.

36. Perpetrators of the particular type of investment fraud scheme detailed below frequently allow victims to withdraw some of their "profits" early in the scheme to engender trust and help convince victims of the legitimacy of the platform. As the scheme continues, victims are unable to withdraw their funds and are provided various excuses as to why. For example, the fraudsters will often refer to a fake "tax" requirement, stating that taxes must be paid on the proceeds generated from the platform. This is just an 11th-hour effort by the fraudsters to elicit more money from victims. Ultimately, victims are locked out of their account and lose all their funds.

37. First employed by Chinese organized crime groups, the particular type of investment fraud scheme detailed below initially targeted victims inside China then expanded worldwide during the global pandemic. Operating from compounds in Cambodia and Myanmar, these criminal syndicates often operate by forcing human trafficking victims in Southeast Asia to participate in the schemes against their will. The schemes take advantage of the ability of cryptocurrency to be transferred securely and globally, without intermediaries and the safeguards established, and inherent to, the traditional financial system.

VI. *N.D. OHIO VICTIM.*

38. On or about June 5, 2024, a victim in the Northern District of Ohio (particularly: Mentor, Ohio) with the initials "A.H." filed a complaint with the FBI's Internet Crime Complaint Center reporting losses from a scam.

39. The incident began when A.H. responded to a text on her phone from an unknown number in November 2023. A.H. began exchanging information about hobbies and religion with her new "friend" ("SUBJECT-1), who A.H. believed to be living in Seattle, Washington. After building a relationship, SUBJECT-1 suggested A.H. invest in cryptocurrencies.

40. Over a period of time, A.H. invested $250,000 of her money, following the instructions from SUBJECT-1 to open an account at Crypto.com and wiring money to the account at that exchange.

41. SUBJECT-1 then instructed A.H. as to what "platform" to use for the investments and where to transfer her purchased cryptocurrency. A.H. transferred the Crypto.com cryptocurrency to the address provided by SUBJECT-1; namely, the cryptocurrency address beginning/ending 0xd95 . . . 4be2cd4.

42. SUBJECT-1 claimed to want to help A.H.'s investment grow and offered to loan A.H. $190,000 to invest. A.H. declined, but SUBJECT-1 insisted, and A.H. eventually relented; so, SUBJECT-1 purportedly added such an amount to A.H.'s invested funds on the "platform".

43. Thinking her initial $250,000 investment was now worth over $1 million, A.H. wanted to withdraw her earnings. SUBJECT-1 encouraged A.H. to do so, presumably knowing A.H. would be asked for additional "fees" to be paid to access her funds.

44. When A.H. attempted to withdraw funds, she was first told a payment of $174,406 was needed to release the funds. A.H. made the payment. A.H. then was told that due to "suspicious activity" and "long-term retention costs" she was required to pay an additional $238,946 in handling fees. A.H. made that payment. After making those two payments, A.H. was told she needed to pay $300,000 to increase her credit score from 85% to 100%, with each point costing $20,000. A.H. did not make this payment as she no longer had any funds left having spent her entire life savings, including her Roth IRA.

45. After A.H. advised SUBJECT-1 she had no money left to give and could not pay back the alleged loan of $190,000, SUBJECT-1 began making threats, telling A.H. that he could send his friends to "take care of" of A.H.'s friends and family.

46. In total, between the initial $250,000 investment and the payment of "fees," A.H. lost approximately $663,352 in the scheme, constituting her entire life savings.

VII. *MICHIGAN, CALIFORNIA, UTAH, AND NORTH CAROLINA VICTIMS.*

47. **"B.D.", a resident of Michigan**, responded to a wrong number text on his phone. B.D. then exchanged texts back and forth with his new "friend" ("SUBJECT-2"), who told him that she was a female living in Seattle, Washington. SUBJECT-2 made promises of meeting B.D. in person, even sending him pictures of a plane ticket for a planned meeting in Chicago,

Illinois. SUBJECT-2 cancelled the meeting before it occurred. After spending time exchanging texts and building a relationship, SUBJECT-2 suggested that B.D. invest in cryptocurrencies.

48. As instructed by SUBJECT-2, B.D. opened accounts at Crypto.com and Kraken and made an initial purchase of cryptocurrency to invest.

49. In or about May 2024, B.D. made an initial "investment" by sending the purchased cryptocurrency to the address provided by SUBJECT-2, which B.D. believed to be the investment platform recommended by SUBJECT-2. To test the reliability of where he was sending funds, B.D. asked for a small withdrawal from the platform, which was successful. Convinced the investment vehicle recommended by SUBJECT-2 was legitimate, B.D. invested more funds.

50. Later, when B.D. attempted to make a withdrawal of his principal and alleged profits, he was told to pay $4,060 to release his funds and cover alleged taxes. B.D. refused to make the payment after the investment platform could not explain how an overseas entity would remit the tax payments to the Internal Revenue Service or to his local taxing authority on his behalf.

51. B.D. lost approximately $11,996 from the investment scheme in which he was directed by SUBJECT-2.

52. **"R.M.", a resident of California**, responded to a wrong number text on his phone in February 2024. R.M. then exchanged texts back and forth with his new "friend" ("SUBJECT-3"), who told him that she was a female living in New York, New York. After spending time exchanging texts and building a relationship, SUBJECT-3 suggested that R.M. invest in cryptocurrencies.

53. As instructed by SUBJECT-3, R.M. opened an account at Crypto.com to make the initial purchase of cryptocurrency to invest. R.M. also opened an account at Coinbase to make purchases for his cryptocurrency "investments".

54. In or about May 2024, R.M. transferred the purchased cryptocurrency to the address recommended by SUBJECT-3, which R.M. believed to be the investment platform. After R.M. was unable to retrieve his funds from the site, he further researched the "investment platform" and learned the website was created the day before he sent over his investment.

55. R.M. lost approximately $234,026 from the investment scheme in which he was directed by SUBJECT-3.

56. **"M.S."**, **a resident of Utah**, responded to a wrong number text on his phone. M.S. then exchanged texts back and forth with his new "friend" ("SUBJECT-4"), who told him that she was a female living in San Francisco, California. After spending time exchanging texts and building a relationship, SUBJECT-4 suggested that M.S. invest in cryptocurrencies.

57. As instructed by SUBJECT-4, M.S. opened an account at Crypto.com to make the initial purchase of cryptocurrency to invest. M.S. also opened an account at Coinbase to make purchases for his cryptocurrency "investments" that were directed by SUBJECT-4.

58. In or about May 2024, M.S. transferred the purchased cryptocurrency to the address recommended by SUBJECT-4, which M.S. believed to be the investment platform recommended by SUBJECT-4. Later, M.S. was unable to retrieve the funds he invested.

59. M.S. lost approximately $136,047 from the investment scheme in which he was directed by SUBJECT-4.

60. **"H.L."**, **a resident of North Carolina**, responded to a wrong number text on her phone in December, 2023. H.L. then exchanged texts back and forth with her new "friend"

("SUBJECT-5"). After spending time exchanging texts and building a relationship, SUBJECT-5 suggested that H.L. invest in cryptocurrencies.

61. As instructed by SUBJECT-5, H.L. opened an account at Crypto.com to make the initial purchase of cryptocurrency to invest. H.L. made purchases of cryptocurrency at Crypto.com and then transferred the funds to an address directed by SUBJECT-5, which H.L. believed to be an investment platform.

62. When H.L. attempted to withdraw the funds from the "investment platform," she was told she had to pay different fees to access her funds.

63. H.L. lost approximately $475,000 from the investment scheme in which she was directed by SUBJECT-5 plus another $165,000 that was provided for the "investment" by a family member, bringing her total loss to approximately $640,000.

64. Funds from A.H., B.D., R.M., M.S., and H.L. were commingled with other funds at various points during the fraudsters' movement and laundering of funds, but - as set forth below - were eventually consolidated at the same address (namely, ADDRESS A-6), indicating that SUBJECT-1 (male), SUBJECT-2 (female), SUBJECT-3 (female), SUBJECT-4 (female), and SUBJECT-5 were acting as part of the same criminal conspiracy operating the investment fraud scheme.

65. In total, A.H., B.D., R.M., M.S., and H.L. lost approximately $1,685,421 in the investment fraud scheme.

VIII. *OTHER VICTIMS.*

66. The above-described victims do not represent the entirety of identified victims. To date, 28 additional victims have been particularly identified. Further, five other victim

accounts have been identified and the FBI is pursuing identifying information for the particular victims. In total, the FBI has identified 38 victims/victim accounts.

67. In total - using either the Last-In, First-Out (LIFO) accounting method, the Proceeds-In, First-Out accounting method, or the First-In, First-Out (FIFO) accounting method - the 28 additional particularly identified victims lost at least $3,260,038 in the investment fraud scheme; and, the victims associated with the five other victim accounts have lost approximately $1,071,086.

68. The identified loss to victims in the instant case exceeds $5.2 million.

IX. *TRACING ANALYSIS.*

69. A.H. (the N.D. Ohio victim) made at least six payments from her account at Crypto.com to the pass-through address beginning/ending 0xd95 . . . 4be2cd4, which A.H. believed to be the "investment platform." From there, funds were then transferred by the fraudsters to unhosted wallet addresses as follows:

a.) On or about May 21, 2024, a transfer of approximately 26.61 ETH ($97,938) [1] to address beginning/ending 0xcf9 . . . b485027 (ADDRESS A-1).

b.) On or about May 17, 2024, a transfer of approximately 33.00 ETH ($97,921) to ADDRESS A-1.

c.) On or about April 30, 2024, a transfer of approximately 15.08 ETH ($48,462) to address beginning/ending 0xe79 . . . c2d6ad0 (ADDRESS B-1).

d.) On or about April 23, 2024, a transfer of approximately 15.27 ETH ($49,086) to ADDRESS B-1.

e.) On or about April 19, 2024, a transfer of approximately 16.14 ETH ($49,496) to address beginning/ending 0xa32 . . . 6f4dbb8 (ADDRESS C-1).

---

[1] When an amount of cryptocurrency is listed in this Complaint in Forfeiture, it sometimes will be followed by a parenthetical approximation of its value in U.S. dollars at the time of the transaction.

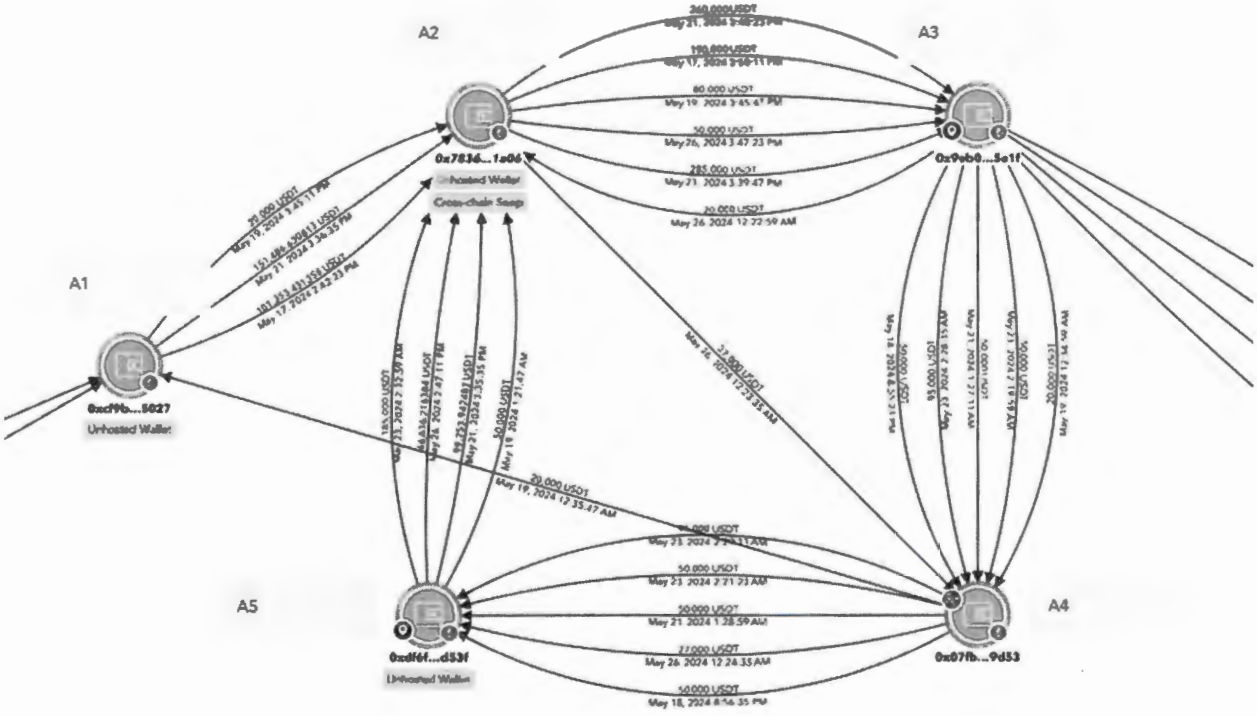
f.) On or about April 2, 2024, a transfer of approximately 8.39 ETH ($29,245) to ADDRESS C-1.

70. The approximately 59.61 ETH ($195,859) of A.H.'s funds that ended up in ADDRESS A-1 were subsequently swapped for Tether ("USDT") cryptocurrency and then transferred to the address beginning/ending 0x783 . . . 2da1a06 (ADDRESS A-2). After arriving in ADDRESS A-2, the funds were broken up multiple times and transferred in a convoluted circular pattern - sometimes multiple times - between ADDRESS A-1, ADDRESS A-2, and three additional addresses as represented below:

a.) address beginning/ending 0x9eb . . . 5db5e1f (ADDRESS A-3).

b.) address beginning/ending 0x07f . . . 93e9d53 (ADDRESS A-4).

c.) address beginning/ending 0xdf6 . . . f0ed53f (ADDRESS A-5).



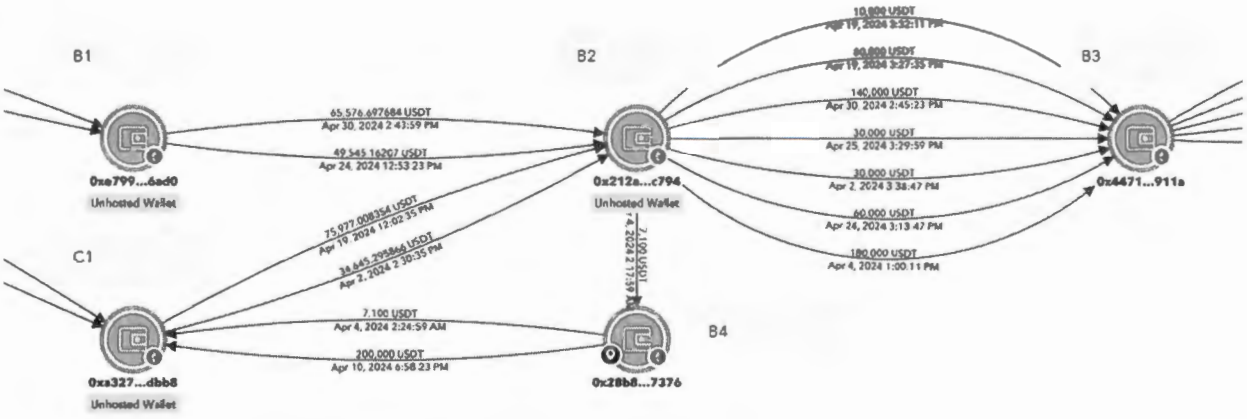
71. Following the transfers set forth above - and using the First-In, First-Out (FIFO) accounting method - the approximately 195,859 USDT ($195,859) of A.H.'s funds ended up at ADDRESS A-3. A.H.'s funds were then transferred as part of four different transfers between approximately May 21, 2024, and May 30, 2024, to the address beginning/ending 0x58e . . . b2d0dcb (ADDRESS A-6).

72. A.H.'s funds (namely, $176,289) that were originally transferred to ADDRESS B-1 and ADDRESS C-1 were swapped for USDT and were involved in a movement of funds between addresses as represented below:

a.) address beginning/ending 0x212 . . . 4d9c794 (ADDRESS B-2).

b.) address beginning/ending 0x447 . . . eb6911a (ADDRESS B-3).

c.) address beginning/ending 0x28b . . . fd17376 (ADDRESS B-4).



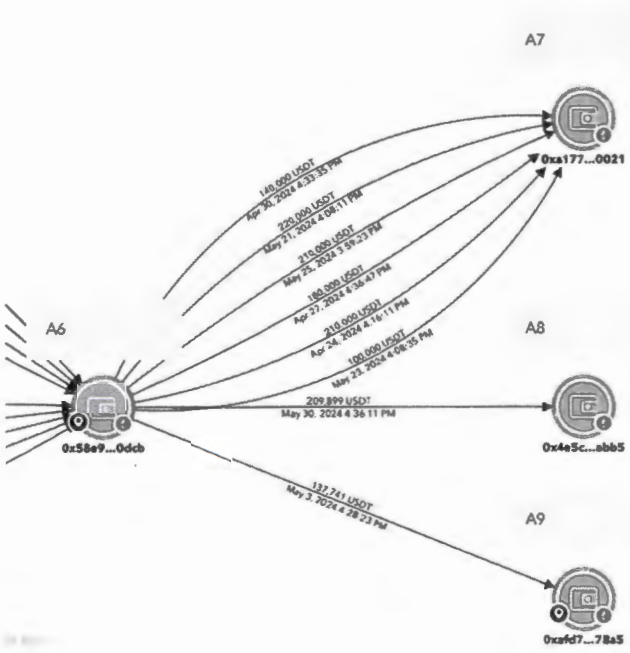
73. Following the transfers set forth in paragraph 72 - and using the First-In, First-Out (FIFO) accounting method - the approximately $176,289 of A.H.'s funds ended up in ADDRESS B-3. Thereafter, the funds were transferred to ADDRESS A-6, the same address where A.H.'s other funds ($195,859) eventually ended up.

74. From ADDRESS A-6, A.H.'s funds were included as represented in the graph below in transfers to the subject three addresses, which received the following approximate amounts:

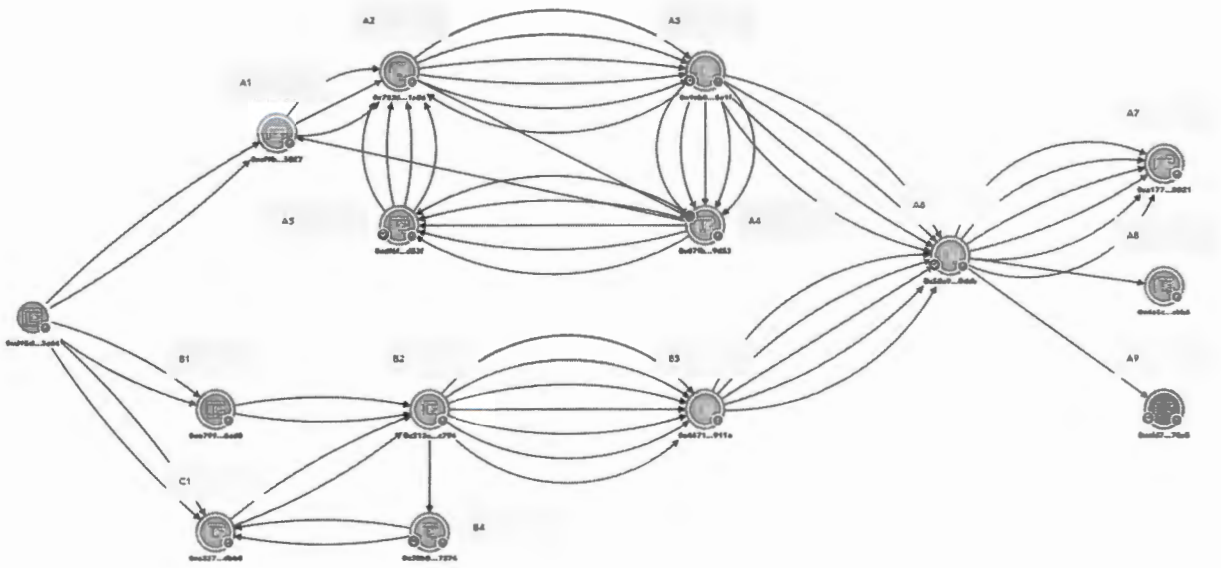
a.) 314,657 USDT ($314,657) to **ADDRESS A-7**.

b.) 11,954 USDT ($11,954) to **ADDRESS A-8**.

c.) 43,071 USDT ($43,071) to **ADDRESS A-9**.



75. The following is a summary graph of the transfers of A.H.'s funds to the subject three addresses:



76. The funds "invested" by B.D. (the Michigan victim - approximately $11,996) followed a similar pattern, in that they were transferred between addresses before being consolidated back at ADDRESS A-6. B.D.'s funds were then included in transfers to the subject three addresses, which received the following approximate amounts:

a.) 5,110 USDT ($5,110) to **ADDRESS A-7**.

b.) 4,967 USDT ($4,967) to **ADDRESS A-8**.

c.) 1,024 USDT ($1,024) to **ADDRESS A-9**.

77. The funds "invested" by R.M. (the California victim - approximately $234,026) followed a similar pattern, in that they were transferred between addresses before being consolidated back at ADDRESS A-6. R.M.'s funds were then included in transfers to two of the subject addresses, which received the following approximate amounts:

a.) 227,963 USDT ($227,963) to **ADDRESS A-7**.

b.) 6,063 USDT ($6,063) to **ADDRESS A-9**.

78. The funds "invested" by M.S. (the Utah victim - approximately $136,047) followed a similar pattern, in that they were transferred between addresses before being consolidated back at ADDRESS A-6. M.S.' funds were then included in transfers to the following subject address, which received the following approximate amount:

a.) 136,047 USDT ($136,047) to **ADDRESS A-8**.

79. H.L. (the North Carolina victim) and her family member "invested"/lost approximately $640,000 in the investment fraud scheme. At least a portion of these funds followed a similar pattern, in that they were transferred between addresses before being consolidated back at ADDRESS A-6. The funds were then included in transfers to two of the subject addresses, which received the following approximate amounts:

a.) 73,619 USDT ($73,619) to **ADDRESS A-7**.

b.) 95,125 USDT ($95,125) to **ADDRESS A-9**.

80. The following is a summary chart of the funds "invested" by A.H., B.D., R.M., M.S., and H.L. that - using the First-In, First-Out (FIFO) accounting method - can be traced to the subject three addresses. In total, **ADDRESS A-7** received approximately $621,349; **ADDRESS A-8** received approximately $152,968; and, **ADDRESS A-9** received approximately $145,283:

Address	A.H. Funds	B.D. Funds	R.M. Funds	M.S. Funds	H.L. Funds
A-7	314,657.00	5,110.00	227,963.00		73,619.00
A-8	11,954.00	4,967.00		136,047.00	
A-9	43,071.00	1,024.00	6,063.00		95,125.00
	369,683.00	**11,101.00**	**234,026.00**	**136,047.00**	**168,744.00**

81. As set forth in paragraph 66 above, A.H., B.D., R.M., M.S., and H.L. do not represent the entirety of victims identified in the investigation. To date, 28 additional victims have been particularly identified. Using either the Last-In, First-Out (LIFO) accounting method, the Proceeds-In, First-Out accounting method, or the First-In, First-Out (FIFO) accounting method, the 28 additional victims had a total of approximately 2,068,942 USDT ($2,068,942) end up in **ADDRESS A-7**; a total of approximately 672,217 USDT ($672,217) end up in **ADDRESS A-8**; and a total of approximately 518,879 USDT ($518,879) end up in **ADDRESS A-9**. These totals are in addition to the amounts detailed for victims A.H., B.D., R.M., M.S., and H.L.

82. Further, again as set forth in paragraph 66, five other victim accounts have been identified, and the FBI is pursuing identifying information for the particular victims. Using the Last-In, First-Out (LIFO) accounting method, these victims had a total of approximately 939,995

USDT ($939,995) end up in **ADDRESS A-8**; and a total of approximately 131,091 USDT ($131,091) end up in **ADDRESS A-9**.

83. In total, approximately 2,690,294 USDT ($2,690,294) of victim funds can be traced to **ADDRESS A-7.** On or about June 21, 2024, the USDT tokens at **ADDRESS A-7** were frozen by Tether Limited.

84. In total, approximately 1,765,180 USDT ($1,765,180) of victim funds can be traced to **ADDRESS A-8.** On or about June 25, 2024, the USDT tokens at **ADDRESS A-8** were frozen by Tether Limited.

85. In total, approximately 795,255 USDT ($795,255) of victim funds can be traced to **ADDRESS A-9.** On or about June 21, 2024, the USDT tokens at **ADDRESS A-9** were frozen by Tether Limited.

86. The identity of the owner(s) of **ADDRESS A-7**, **ADDRESS A-8**, and **ADDRESS A-9** are unknown. The only available information to law enforcement is the cryptocurrency addresses themselves. Notice of this action will be messaged via the Ethereum blockchain to the addresses with a link to a copy of this Complaint in Forfeiture.

X. *CONCLUSION.*

87. Based upon the foregoing, all funds in ADDRESS A-7, ADDRESS A-8, and ADDRESS A-9 are proceeds of wire fraud/conspiracy to commit wire fraud and, accordingly, are subject to forfeiture to the United States under 18 U.S.C. Section 981(a)(1)(C). In addition to the funds stolen from the above-described 38 victims, any other USDT in ADDRESS A-7, ADDRESS A-8, and/or ADDRESS A-9 appear to be the proceeds of fraud. To date, the investigation has not uncovered any indication that the possessor(s) of the funds described above were engaged in legitimate activity, business or otherwise.

88. The transfers of USDT to ADDRESS A-7, ADDRESS A-8, and ADDRESS A-9 described above constituted monetary transactions in violation of 18 U.S.C. Section 1957 (transactional money laundering). Under 18 U.S.C. Section 981(a)(1)(A), all property - real and personal - "involved in" or traceable to an offense in violation of § 1957 is subject to forfeiture. Under § 1957, the SUA proceeds in the transfers - along with any "other funds" transferred with the SUA proceeds - are all forfeitable as the corpus of the money laundering offenses.

89. The transfers to ADDRESS A-7, ADDRESS A-8, and ADDRESS A-9 also constituted transactions in violation of 18 U.S.C. Section 1956(a)(1)(B)(i) (concealment money laundering). The blockchain analysis in this case demonstrated that the fraudsters moved the proceeds of the criminal activity through multiple financial accounts, sometimes at a rapid pace, with no discernable legitimate purpose. Such convoluted transactions that serve no apparent legitimate purpose imply that the purpose of the convoluted transactions was to conceal the nature, source, location, ownership, and control of the SUA proceeds.

90. Under 18 U.S.C. Section 981(a)(1)(A), all property - real and personal - "involved in" or traceable to an offense in violation of § 1956(a)(1)(B)(i) is subject to forfeiture. Particularly, "other funds" in a cryptocurrency address into which SUA proceeds are transferred as part of a concealment money laundering offense - along with any "other funds" transferred with the SUA proceeds as part of the concealment money laundering offense - are subject to forfeiture as property "involved in" the offense. In both instances, the "other funds" commingled with the SUA proceeds obfuscate the origin or existence of the SUA proceeds. Therefore, all funds in ADDRESS A-7, ADDRESS A-8, and ADDRESS A-9 were "involved in" concealment money laundering.

91. Finally, in a money laundering conspiracy case under 18 U.S.C. Section 1956(h), all properties involved in the course of conduct constituting the money laundering conspiracy - including "other funds" - are subject to forfeiture. On this additional basis, all funds in ADDRESS A-7, ADDRESS A-8, and ADDRESS A-9 are subject to forfeiture to the United States under 18 U.S.C. Section 981(a)(1)(A).

WHEREFORE, plaintiff, the United States of America, requests that the Court enter judgment condemning the defendant properties and forfeiting them to the United States, and providing that the defendant properties be delivered into the custody of the United States for disposition in accordance with law and for such other relief as this Court may deem proper.

Respectfully submitted,

Carol M. Skutnik
Acting United States Attorney, N.D. Ohio

By: _____
James L. Morford (Ohio: 0005657)
Assistant United States Attorney, N.D. Ohio
Carl B. Stokes U.S. Court House
801 West Superior Avenue, Suite 400
Cleveland, Ohio 44113
216.622.3743 / James.Morford@usdoj.gov

VERIFICATION

STATE OF OHIO)
) SS.
COUNTY OF CUYAHOGA)

I, James L. Morford, under penalty of perjury, depose and say that I am an Assistant United States Attorney for the Northern District of Ohio, and the attorney for the plaintiff in the within entitled action. The foregoing Complaint in Forfeiture is based upon information officially provided to me and, to my knowledge and belief, is true and correct.

James L. Morford (Ohio: 0005657)
Assistant United States Attorney, N.D. Ohio

Sworn to and subscribed in my presence this 25th day of February, 2025.

Notary Public

ANNA J DUDAS
Notary Public
State of Ohio
My Comm. Expires
December 5, 2026