IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF OHIO

EASTERN DIVISION

UNITED STATES OF AMERICA,	)	CASE NO.
	)	
Plaintiff,	)	
	)	JUDGE
v.	)	
	)	
947,883 TETHER ("USDT") CRYPTOCURRENCY, VALUED AT APPROXIMATELY $947,883.00, FORMERLY ASSOCIATED WITH CRYPTOCURRENCY ADDRESS BEGINNING/ENDING 0x7d5 . . . 48a8306,	)	
	)	
Defendant.	)	**COMPLAINT IN FORFEITURE**

NOW COMES plaintiff, the United States of America, by its attorneys, Rebecca C. Lutzko, 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 property pursuant to: (i) 28 U.S.C. Section 1355(b)(1)(A) because acts giving rise to the forfeiture occurred in this district; (ii) 28 U.S.C. Section 1355(b)(1)(B), incorporating 28 U.S.C. Section 1395, because the action accrued in this district; and, (iii) 28 U.S.C. Section 1355(b)(1)(B), incorporating 28 U.S.C. Section 1395, because - following the issuance of the seizure warrant - Tether Limited Inc. transferred the defendant property to a government-controlled wallet housed in this district.

3. The defendant property is presently in the custody of the United States Marshals Service (USMS). This Court will have control over the defendant property through service of an arrest warrant *in rem*, which the USMS will execute upon the defendant property. *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; (ii) 28 U.S.C. Section 1395 because the action accrued in this district; and, (iii) 28 U.S.C. Section 1395 because - following the issuance of the seizure warrant - Tether Limited Inc. transferred the defendant property to a government-controlled wallet housed in this district.

5. The defendant property is 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 property also is 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 1957 (sometimes referred to as transactional money laundering), 18 U.S.C. Section 1956(a)(1)(B)(i) (sometimes referred to as concealment 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 PROPERTY.*

7. The following property is the defendant property in the instant case:

947,883 Tether ("USDT") cryptocurrency, valued at approximately $947,883.00, formerly associated with the cryptocurrency address beginning/ending 0x7d5 . . . 48a8306 on the Ethereum blockchain. On or about December 21, 2023, 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 Jennifer D. Armstrong on July 31, 2024, Tether Limited "burned" the USDT tokens associated with the cryptocurrency address and reissued the equivalent amount of USDT tokens [namely, 947,883 USDT] to a U.S. law enforcement-controlled virtual currency wallet. The cryptocurrency address beginning/ending 0x7d5 . . . 48a8306 is referred to in the following paragraphs as "ADDRESS-7."

III. *STATUTES.*

8. <u>Offense Statutes</u>. This Complaint in Forfeiture relates to violations of 18 U.S.C. Section 1343 (wire fraud), 18 U.S.C. Sections 1957 and 1956 (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 [§ 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."

11. **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."

12. 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 1957 (transactional money laundering) and/or 18 U.S.C. Section 1956(a)(1)(B)(i) (concealment money laundering) is subject to forfeiture.

13. 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.

14. **"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.

15. **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.

IV. *BACKGROUND ON CRYPTOCURRENCY.*

16. *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.

17. *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.

18. *DAI*: Like USDT, DAI is a blockchain-based cryptocurrency that is tied - or tethered - to fiat currencies. DAI is pegged to the U.S. Dollar at a 1:1 ratio. Unlike centralized stablecoins, DAI is not backed by fiat currency and other assets held by the issuer. Instead, DAI is backed by digital collateral on the Maker cryptocurrency platform.

19. *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.

20. *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’s private key can authorize a transfer of virtual currency from that address to another address.

21. *Virtual Currency Wallet*: There are various types of virtual currency wallets, including software wallets, hardware wallets, and paper wallets. A software wallet is a software application that interfaces with the virtual currency’s specific blockchain and generates and stores a user’s address(es) 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.

22. *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.

23. *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.

24. *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.

25. *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.

26. *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.

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

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

V. *BACKGROUND OF INVESTIGATION.*

29. 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.

30. These schemes often begin in a number of ways, such as a misdialed text to WhatsApp message or making a connection online with a new person via a social media or dating website. From there, the scammer will attempt to establish a more personal relationship with the victim by using manipulative tactics expressing care and concern for the victim before making escalating requests for money, often via cryptocurrency.

31. On or about October 20, 2023, a victim in Elyria, Ohio, with the initials "J.S." filed a complaint with the FBI's Internet Crime Complaint Center reporting losses from a computer tech scam.

32. The incident began when J.S. noticed an alert on his Macbook laptop screen telling him his computer was compromised and telling him to call a telephone number to resolve the issue. An individual using the suspected alias "Allan Walton" ("Walton") answered the

telephone stating that he was an Apple employee, and falsely stating that J.S.'s retirement account at his financial institution ("financial institution-1") had been compromised.

33. While on the telephone with J.S., Walton added an individual using the suspected alias "Stephen Gruber" ("Gruber"), who claimed to be the senior risk and fraud analyst employee on the case regarding J.S.'s computer.

34. Gruber falsely told J.S. that three separate transactions - in the amounts of $23,152.00, $31,421.67, and $36,278.71 - had taken place moving money from J.S.'s account at financial institution-1. Gruber told J.S. that the recipients of the claimed transfers were in either China or Russia, in addition to one going directly to a casino in Las Vegas. Gruber advised J.S. that the transaction sent to the casino could potentially be stopped with the assistance of the Federal Trade Commission. Gruber told J.S. that to keep his money safe, J.S. would need to wire money at the direction of Gruber and/or Walton.

35. Walton instructed J.S. to download a screen sharing service onto his Macbook. This gave Walton access to J.S.'s computer. Using this access, Walton created an account at a virtual currency exchange (VCE-1) using the email account s******j***465@gmail.com.[1]

36. On two separate occasions, Walton then directed J.S. to wire funds to the newly created account at VCE-1 from J.S.'s personal bank account at another financial institution ("financial institution-2").

37. On or about October 18, 2023, J.S. wired $145,000.00 into the newly created account at VCE-1 via his personal account at financial institution-2. On or about October 19, 2023, a confirmation email was sent to s******j***465@gmail.com from VCE-1 confirming

[1] To ensure the integrity of the FBI's investigation, and to reduce the risk of anyone inadvertently e-mailing the target(s) of the investigation, portions of e-mail addresses are replaced with asterisks throughout this Complaint in Forfeiture.

the deposit of $145,000.00 credited to J.S.'s cryptocurrency wallet held at VCE-1; address beginning/ending: 0x4FA . . . e991a3d (ADDRESS-1).

38. On or about October 19, 2023, using his control of J.S.'s Macbook via the screen sharing software, Walton withdrew approximately 84.98 Ethereum ($133,749.00) [2] from J.S.'s account at VCE-1. Publicly available websites confirm this transaction took place on the Ethereum blockchain with transaction hash: 0x905b13d60812cc54ca2f9fdc8d1795f81d0ed8048387955c04b60113cdf48453.

39. On or about October 20, 2023, at the direction of Gruber and/or Walton, J.S. wired $115,000.00 into the newly created account at VCE-1 via his personal account at financial institution-2. On or about October 20, 2023, a confirmation email was sent to s******j***465@gmail.com from VCE-1, confirming the deposit of $115,000.00 credited to J.S.'s cryptocurrency wallet held at ADDRESS-1.

40. On or about October 23, 2023, using his control of J.S.'s Macbook via the screen sharing software, Walton withdrew approximately 75 Ethereum ($120,000.00) from J.S.'s account at VCE-1. Publicly available websites confirm this transaction took place on the Ethereum blockchain with transaction hash: 0x7ea06e4f7ca9656cb26ed0098f9f02f66032ef9b781df752272e459de0dd90b6.

41. On or about November 1, 2023, at the direction of Gruber and/or Walton, J.S. wired approximately $165,000.00 to a different virtual currency exchange (VCE-2) from J.S.'s personal account at financial institution-2, where it was converted to Tether (USDT).

[2] 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.

42. On or about November 2, 2023, using his control of J.S.'s Macbook via the screen sharing software, Walton took approximately $155,093.00 worth of the $165,000.00 that was converted to USDT at VCE-2 and transferred it to ADDRESS-1. Publicly available websites confirm this transaction took place on the Ethereum blockchain with transaction hash: 0x9a06ad4a9aed9afe44ea1dbadc002e50dcf53804cbd2ec1e9b1855e385aa36ad.

43. On or about November 2, 2023, using his control of J.S.'s Macbook via the screen sharing software, Walton withdrew approximately 155,093 USDT ($155,093.00) from ADDRESS-1. Publicly available websites confirm this transaction took place on the Ethereum blockchain with transaction hash: 0x070ec45283708148f2501f8bee8fdfd43650b9ca5e11624f8c15b5ba517cef53.

44. After the transactions to ADDRESS-1 were completed, J.S. called financial institution-1 to ask about the wires Walton claimed were sent to China, Russia, and the casino in Las Vegas. The employee at financial institution-1 advised J.S. that the transactions never occurred.

45. As a result of the cryptocurrency fraud scam, J.S. - a senior citizen - lost his entire life savings. J.S. and his wife are currently living off Social Security and assistance from a relative.

VI. TRACING ANALYSIS.

46. As set forth at paragraph 38, above - and using the access and control he had of J.S.'s computer - Walton withdrew 84.98 ETH ($133,749.00) from ADDRESS-1 on or about October 19, 2023. As stated, ADDRESS-1 was the address owned and funded by J.S. at VCE-1.

47. Of this 84.98 ETH ($133,749.00), the Federal Bureau of Investigation (FBI) was able to trace approximately $105,615.00 of J.S.'s funds to ADDRESS-7. On or about December 21, 2023, the cryptocurrency at ADDRESS-7 was frozen by Tether Limited.

48. The FBI's tracing analysis - using the First-In First-Out (FIFO) accounting methodology - is as follows:

A. On or about October 19, 2023, the 84.98 ETH ($133,749.00) was moved from J.S.'s wallet to the unhosted wallet address beginning/ending: 0xe2b . . . b1c12f9 (ADDRESS-2). At the time of this transfer into ADDRESS-2, there was no other ETH contained in ADDRESS-2.

B. The next transaction by ADDRESS-2 was the swap of ETH for 132,259 Tether ("USDT") ($132,259.00). The value of the ETH at the time of the transaction was $133,749.00. After the swap - on AirSwap - ADDRESS-2 ended up with $132,259.00 worth of USDT. Based on the exchange rate available on AirSwap and fees assessed, the individual executing this transaction suffered an economic cost of approximately $1,500.00 solely to have a different version of cryptocurrency.

C. At the time of the swap, ADDRESS-2 had a pre-existing balance of approximately 268,891 USDT ($268,891.00). After the swap, the balance was 401,151 USDT ($401,151.00). Using the FIFO accounting methodology, the funds from J.S. in the wallet were the USDT from 268,891 to 401,151. After the funds belonging to J.S. were deposited into ADDRESS-2, additional USDT was added to the wallet bringing the total to 793,371 USDT.

D. On or about October 20, 2023, a total of 793,371 USDT ($793,371.00) was transferred from ADDRESS-2 to the wallet address beginning/ending: 0x61d . . . f7bf98d (ADDRESS-3), with the 132,259 USDT ($132,259.00) that originated in J.S.'s account included.

At the time of the transfer into ADDRESS-3, there was no other USDT contained in ADDRESS-3. Using the FIFO accounting methodology, the funds from J.S. represented the USDT in ADDRESS-3 from 268,891 to 401,151.

E. The next USDT transaction by ADDRESS-3 was the swap of 555,000 USDT for 555,563 DAI ("DAI"). Of this 555,563 DAI, the funds from J.S. represented the DAI from 268,891 to 401,151. However, at the time of the swap, ADDRESS-3 had a pre-existing balance of approximately 305,162 DAI. Therefore, using the FIFO accounting methodology, the funds from J.S. represented the DAI in ADDRESS-3 from 574,054 to 706,314.

F. After the funds belonging to J.S. were deposited into ADDRESS-3, additional DAI was added to the wallet, bringing the eventual total to 1,071,113 DAI, with the funds from J.S. still representing the DAI in ADDRESS-3 from 574,054 to 706,314.

G. On or about November 23, 2023, there was a transfer of 600,000 DAI ($600,000.00) to another address. Using the FIFO accounting methodology, that transfer included 25,945 of the DAI belonging to J.S. After the November 23, 2023 transaction, 471,113 DAI remained in ADDRESS-3. Using the FIFO accounting methodology, the portion of funds from J.S. represented the DAI from 0 to 106,314 in ADDRESS-3.

H. On or about December 14, 2023, a total of 421,247 DAI ($421,247.00) was transferred from ADDRESS-3 to the wallet address beginning/ending: 0x422 . . . b0c4481 (ADDRESS-4), with the 106,314 DAI belonging to J.S. included. At the time of the transfer, ADDRESS-4 had a pre-existing balance of approximately 301 DAI. Using the FIFO accounting methodology, the funds from J.S. in ADDRESS-4 represented the DAI from 301 to 106,615.

I. The next DAI transaction on ADDRESS-4 was the swap of 1,000 DAI for 0.43 ETH, which included 699 DAI that can be traced to funds from J.S. The ETH from this swap was then used to fund fees on the Ethereum Network; *i.e.*, to help pay for subsequent transactions, to include those from ADDRESS-4 to ADDRESS-5.

J. The next DAI transaction on ADDRESS-4 was the swap of 10,000 DAI for 9,978 ($9,978.00) USDT. Using the FIFO accounting methodology, all of the DAI in this swap represented funds from J.S. Prior to the swap, ADDRESS-4 had a balance of approximately 0 USDT ($0.00). After the swap, using the FIFO accounting methodology, the USDT funds in ADDRESS-4 from J.S. represented the USDT from 0 to 9,978.

K. The next transaction on ADDRESS-4 was the transfer of 9,978 USDT ($9,978.00) on or about December 14, 2023, to the wallet address beginning/ending: 0x12e . . . 2703125 (ADDRESS-5).

L. As cryptocurrency transactions are not reversible, address owners will often send a test transaction of a smaller amount to ensure that it goes through before sending a larger amount to the same address. The transfer of the "small amount" of 9,978 USDT from ADDRESS-4 to ADDRESS-5 on or about December 14, 2023, appears to be such a test transaction.

M. The next DAI transaction on ADDRESS-4 - after the swap of the 10,000 DAI for 9,978 USDT set forth in paragraph 48(J) - was the swap of 410,000 DAI for 410,431 USDT. Prior to the swap, ADDRESS-4 had a balance of approximately 0 USDT ($0.00). After the swap, using the FIFO accounting methodology, the funds in ADDRESS-4 from J.S. represented the USDT from 0 to 95,636 out of the total 410,431 USDT.

N. Moving cryptocurrency from one stablecoin (USDT) to another (DAI) and back again in a short time would be an extremely unusual investment strategy as both USDT and DAI strive to reflect a value on par with a 1:1 ratio with the U.S. Dollar and, therefore, have only minor fluctuations in value. Given the fees and costs incurred for each transaction, it is unlikely that this strategy would ever profit an investor. Therefore, the most likely reason for these transactions was to engage in concealment money laundering of stolen funds.

O. The next USDT transaction on ADDRESS-4 was the transfer of 387,287 USDT ($387,287.00) on or about December 14, 2023 to ADDRESS-5. Using the FIFO accounting methodology, that transfer included the 95,636 USDT ($95,636.00) belonging to J.S.

P. ADDRESS-5 had a pre-existing balance of approximately 9,889 USDT before the transfer in of the 9,978 USDT belonging to J.S., which was described in paragraph 48(K). Using the FIFO accounting methodology, the funds in ADDRESS-5 from J.S. represented the USDT from 9,890 to 19,867. After the 387,287 USDT transfer set forth in paragraph 48(O) - of which the first 95,636 were funds that originated in J.S.'s account - the balance in ADDRESS-5 was 407,155 USDT. After this second transfer from ADDRESS-4 - using the FIFO accounting methodology - the funds in ADDRESS-5 from J.S. represented the USDT from 9,890 to 115,504.

Q. On or about December 14, 2023, a total of approximately 407,000 USDT ($407,000.00) was transferred from ADDRESS-5 to the wallet address beginning/ending: 0xa6e . . . 2473f64 (ADDRESS-6), including the 105,615 USDT ($105,615.00) that originated in J.S.'s account. There was a balance of less than 1 USDT ($0.00) in ADDRESS-6 before the transfer from ADDRESS-5. After the transfer from ADDRESS-5 - using the FIFO accounting methodology - the funds from J.S. represented the USDT from 9,891 to 115,505 in ADDRESS-6.

R. On or about December 14, 2023, a total of approximately 355,077 USDT was transferred from ADDRESS-6 to the wallet address beginning/ending: 0x7d5 . . . 48a8306

(ADDRESS-7), including the 105,615 USDT ($105,615.00) that originated in J.S.'s account. At the time of the transfer, ADDRESS-7 had a pre-existing balance of approximately 732,738 USDT. After the transfer, ADDRESS-7 had a balance of approximately 1,087,815 USDT.

S. Between December 14, 2023 and December 21, 2023, approximately 139,921 USDT was transferred out of ADDRESS-7.

T. On or about December 21, 2023, the USDT at ADDRESS-7 was frozen by Tether Limited. At the time of the freeze, ADDRESS-7 had a balance of approximately 947,883 USDT.

U. Approximately $105,615.00 of the funds that J.S. believed he was sending to protect funds in his retirement account ended up in ADDRESS-7.

VII. *CONCLUSION.*

49. The transfer of the 355,077 USDT ($355,077.00) on December 14, 2023, from ADDRESS-6 into ADDRESS-7 constituted a monetary transaction 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. As set forth in paragraph 48(R), the transfer of the 355,077 USDT into ADDRESS-7 on December 14, 2023, involved the 105,615 USDT belonging to J.S. and other funds commingled with the 105,615 USDT. Under § 1957, the entire 355,077 USDT is forfeitable as the corpus of the money laundering offense.

50. The transfer of the 355,077 USDT on December 14, 2023, from ADDRESS-6 into ADDRESS-7 also constituted a transaction in violation of 18 U.S.C. Section 1956(a)(1)(B)(i) (concealment money laundering). At the time of the transfer, ADDRESS-7 had a pre-existing balance of approximately 732,738 USDT.

51. 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.

52. Under 18 U.S.C. Section 981(a)(1)(A), the entire defendant property - namely, 947,883 USDT ($947,883.00) - is forfeitable. The "other funds" that were commingled with the 105,615 USDT belonging to J.S. in the December 14, 2023, transfer of approximately 355,077 USDT from ADDRESS-6 to ADDRESS-7 - and the pre-existing balance of approximately 732,738 USDT in ADDRESS-7 - also were "involved in" the concealment money laundering offense and, accordingly, are subject to forfeiture in that they facilitated the violation by helping to conceal the nature, source, ownership, and/or control of the USDT traceable to J.S.

53. The entire defendant property - namely, 947,883 USDT ($947,883.00) - also is subject to forfeiture 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" - 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. In addition to the funds stolen from J.S., the other USDT funds seized from ADDRESS-7 appear to be the proceeds of fraud in that they bear the hallmarks of similar money laundering activity - with no economic purpose - before being deposited into ADDRESS-7.

WHEREFORE, plaintiff, the United States of America, requests that the Court enter judgment condemning the defendant property and forfeiting it to the United States, and providing that the defendant property 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,

Rebecca C. Lutzko
U.S. Attorney, Northern District of 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 25 day of November, 2024.

Anna J Dudas
Notary Public

NOTARY PUBLIC STATE OF OHIO

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