

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF OHIO  
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	CASE NO. 4:25-CV-1780
	)	
Plaintiff,	)	
	)	CHIEF JUDGE SARA LIOI
v.	)	
	)	
325,060 TETHER ("USDT")	)	
CRYPTOCURRENCY, VALUED AT	)	
APPROXIMATELY \$325,060, FORMERLY	)	
ASSOCIATED WITH CRYPTOCURRENCY	)	
ADDRESS BEGINNING/ENDING	)	
TUpj2 . . . LaDkkMB,	)	
	)	
Defendant.	)	<b>COMPLAINT IN FORFEITURE</b>

NOW COMES plaintiff, the United States of America, by its attorneys, David M. Toepfer, United States Attorney for the Northern District of Ohio, and James L. Morford, Assistant U.S. 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; 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 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; and (ii) 28 U.S.C. Section 1395 because the action accrued 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 wire fraud conspiracy, 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 1956(a)(1)(B)(i) (sometimes referred to as concealment money laundering), 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:

325,060 Tether ("USDT") cryptocurrency - valued at approximately \$325,060 - formerly associated with the cryptocurrency address beginning/ending TUpj2 . . .

LaDkkMB on the Tron blockchain. On or about December 31, 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 Carmen E. Henderson on March 20, 2025, Tether Limited “burned” the USDT tokens associated with the cryptocurrency address and reissued the equivalent amount of USDT tokens [namely, 325,060 USDT] to a U.S. law enforcement-controlled virtual currency wallet. The cryptocurrency address beginning/ending TUpj2 . . . LaDkkMB is referred to in the following paragraphs as “**ADDRESS-8.**”

### 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. Section 371 (wire fraud conspiracy), and 18 U.S.C. Section 1956 (money laundering).

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. *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) is subject to forfeiture.

12. 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.

13. *“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.

14. *Facilitation of a Laundering Transaction*:

a.) Individuals engaged in fraud sometimes move proceeds of criminal activity through multiple financial accounts, sometimes at a rapid pace, and often with no discernable legitimate purpose. Such convoluted transactions that serve no apparent legitimate purpose can imply that the purpose of those convoluted transactions was to conceal the nature, source, location, ownership, and/or control of the victim’s proceeds.

b.) “Other funds” that facilitate such money laundering conduct - by helping conceal the nature, source, ownership, or control of the cryptocurrency traceable to a fraud victim(s) - 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.*

15. *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.

16. *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.

17. *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.

18. *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 key(s). 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.

19. *Hosted and Unhosted 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. 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.

20. *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.

21. *Blockchain:* Many virtual currencies publicly record all 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.

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 address on a particular blockchain. A blockchain explorer is software that uses API<sup>1</sup> 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. For all cryptocurrency transactions detailed herein, dates, times, amounts, and valuations are all approximations.

V. *BACKGROUND OF INVESTIGATION.*

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

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

26. Based on data submitted to the FBI's Internet Crime Complaint Center in 2024, the particular type of investment fraud scheme detailed below targeted tens of thousands of victims in the United States and resulted in over \$5.8 billion in private assets being siphoned overseas. The scheme begins with 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.

27. 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.

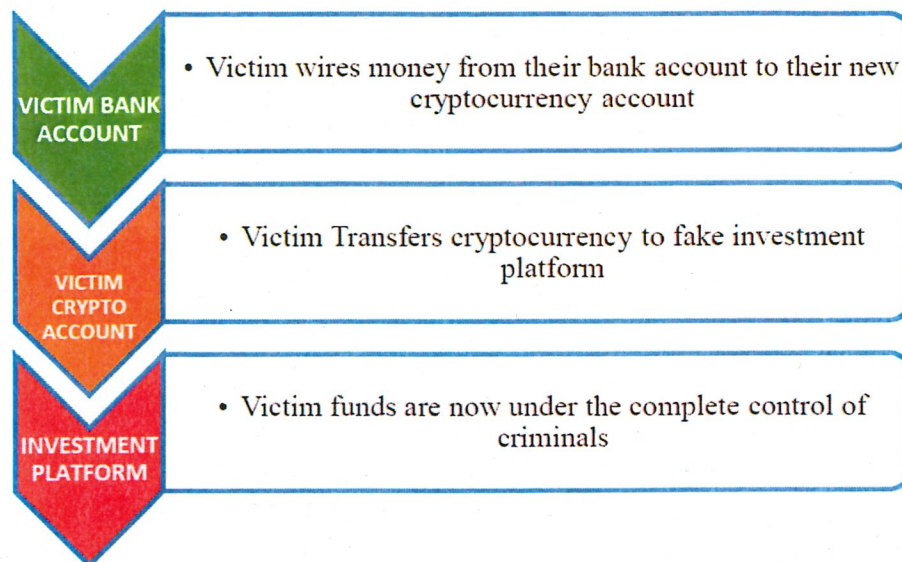
---

<sup>1</sup> API stands for application programming interface, which is a set of definitions and protocols for building and integrating application software.



28. 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.

29. 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.



30. 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 eleventh-hour effort by the fraudsters to elicit more money from victims. Ultimately, victims are locked out of their account and lose all their funds.

31. 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 that are established, and inherent to, the traditional financial system.

VI. *N.D. OHIO VICTIM.*

32. On or about November 24, 2024, an elderly male victim in Bristolville, Trumbull County, Ohio - with the initials "J.K." - filed a complaint with the FBI's Internet Crime Complaint Center. The fraud began when J.K. received a text from an unknown number looking for someone named "Zach." When J.K. responded to the wrong number, he began exchanging information with his new "friend" ("SUBJECT-1"). SUBJECT-1 suggested that they move their exchanges to the messaging platform Telegram, where her username was displayed as "Shaw Goddess". After building a relationship and establishing herself to J.K. as a successful investor, SUBJECT-1 suggested J.K. invest in cryptocurrencies at her direction.

33. SUBJECT-1 directed J.K. to open an account at Crypto.com, a virtual currency exchange (VCE). J.K. did not have an account with Crypto.com before opening one at SUBJECT-1's direction. Eventually, Crypto.com limited the amount of cryptocurrency J.K. could purchase using the account, and SUBJECT-1 instructed J.K. to open an account at

Strike.com, another VCE. In total, J.K. wired over \$1 million to his VCE accounts at Crypto.com and Strike.com. SUBJECT-1 then instructed J.K. as to what (fake) investment platform to use for the “investments” and where to transfer his cryptocurrency purchased at Crypto.com and Strike.com.

34. Before making larger investments, J.K. tested the (fake) investment platform’s legitimacy by requesting multiple returns of a portion of funds from his first few investments. After the requests were processed successfully and funds were returned to J.K., J.K. was convinced that the investment platform was legitimate and continued with larger additional “investments”.

35. J.K. convinced his sister - initials “L.D.” - to make investments that totaled over \$600,000.00 as well.<sup>2</sup>

36. J.K. tried to withdraw some of his later alleged gains from the (fake) investment platform. He was told that his funds were in “lock-up mining” and could not be withdrawn. Around that same time, his sister (L.D.) tried making a withdrawal and was told that a 10% tax had to be paid upfront, which eventually would be credited back to the account of L.D. That concerned J.K., as he knew how taxation worked and this was inconsistent with his understanding. Those two events gave J.K. the realization that he was the victim of a fraud scheme.

---

<sup>2</sup> Although - as set forth below - the FBI was able to trace approximately \$198,950.00 of J.K.’s funds to **ADDRESS-8**, none of L.D.’s funds ended up in **ADDRESS-8**. Accordingly, no portion of L.D.’s “investment” is recoverable in this case.



VII. *FORFEITURE OF ALL TETHER ("USDT") CRYPTOCURRENCY (NAMELY, APPROXIMATELY 325,060 USDT VALUED AT APPROXIMATELY \$325,060) FORMERLY HELD AT ADDRESS-8 ON THE TRON BLOCKCHAIN.*

37. Of the approximately \$1 million "invested" by J.K., the FBI was able to trace approximately \$198,950 of his funds to **ADDRESS-8** as follows:

38. From May 8, 2024 through May 28, 2024, J.K. made at least 12 transfers of BTC from his accounts at Crypto.com and Strike.com - either directly or indirectly (*i.e.*, through a pass-through address) - to the fake investment platform with address beginning/ending 371PVp . . . D5dT (ADDRESS-1). These transfers totaled 2.9859019 BTC (\$195,832):

- |  |   |
|--|---|
| a.) May 8 - 0.3873 BTC (\$24,284) <sup>3</sup> | b.) May 13 - 0.234592 BTC (\$14,460)    |
| c.) May 14 - 0.264459 BTC (\$16,683)           | d.) May 15 - 0.251883 BTC (\$15,518)    |
| e.) May 16 - 0.247995 BTC (\$16,419)           | f.) May 17 - 0.24361025 BTC (\$15,913)  |
| g.) May 17 - 0.144388 BTC (\$9,432)            | h.) May 23 - 0.02528904 BTC (\$1,758)   |
| i.) May 23 - 0.2495857 BTC (\$16,893)          | j.) May 24 - 0.21659115 BTC (\$14,714)  |
| k.) May 25 - 0.14008 BTC (\$9,610)             | l.) May 28 - 0.58012876 BTC (\$40,148). |

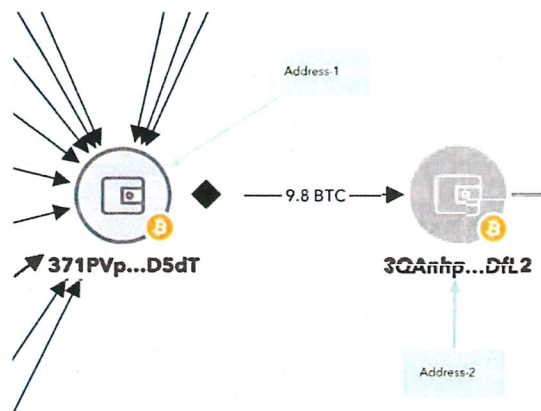
39. When the funds were received at ADDRESS-1, the theft of J.K.'s funds was complete. The funds were under the custody and control of the fraudsters.

40. The approximately 2.9859019 BTC of J.K.'s funds was aggregated in ADDRESS-1, then transferred out with other funds, which appear to be funds derived from similar fraudulent activity. The transfer - on June 5, 2024 - involved a total of approximately 9.8

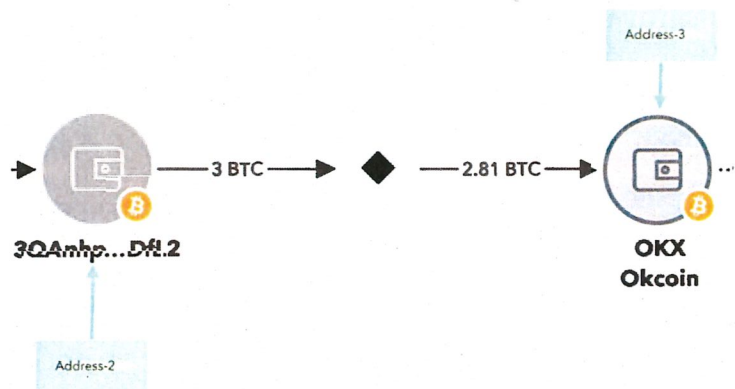
---

<sup>3</sup> 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.

BTC and was sent to the address beginning/ending 3QAnhp . . . DfL2 (ADDRESS-2). Using the Proceeds In, First Out tracing methodology, 2.9859019 BTC of the funds belonged to J.K.:



41. That same day - June 5, 2024 - approximately 2.81 BTC was transferred out of ADDRESS-2 and sent to ADDRESS-3, an address controlled by OKX - a virtual currency exchange (VCE). Using the Proceeds In, First Out tracing methodology, the transfer of the 2.81 BTC consisted entirely of funds belonging to J.K.:



42. ADDRESS-3 is associated with an individual from Cambodia. As set forth above, perpetrators of the particular type of investment fraud scheme carried out in this case often operate out of Cambodia and Myanmar.

43. Within the account at OKX (ADDRESS-3), the approximately 2.81 BTC was swapped for Tether (“USDT”) cryptocurrency,<sup>4</sup> with the account receiving approximately 198,954.27 USDT (\$198,954) in return. Less than three hours later, approximately 198,953.27 USDT (\$198,953) was transferred out of the OKX account to the address beginning/ending TSHWYe . . . boNs (ADDRESS-4). Using the Proceeds In, First Out tracing methodology, the approximately 198,953.27 USDT transferred to ADDRESS-4 was all funds that belonged to J.K.:



44. ADDRESS-4 is known to be used by bad actors to launder and obfuscate the movement of funds on the blockchain. Approximately 98% of the incoming transfers to ADDRESS-4 are from OKX - the same VCE used in the instant fraud scheme regarding J.K. - to exchange BTC for USDT. In tracing funds from multiple complaints made to the FBI - including two other victims from the Northern District of Ohio and a complaint made to a local police department in rural Illinois - law enforcement has identified ADDRESS-4 as being

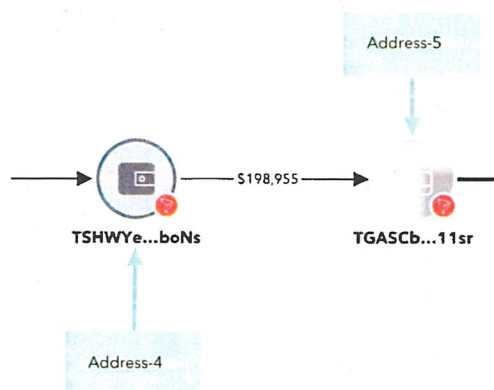
---

<sup>4</sup> Tether (USDT) is a “stablecoin,” a type of blockchain-based virtual currency that is tied - or tethered - to a fiat currency. USDT exists on several third-party blockchains, including the Tron blockchain. 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.

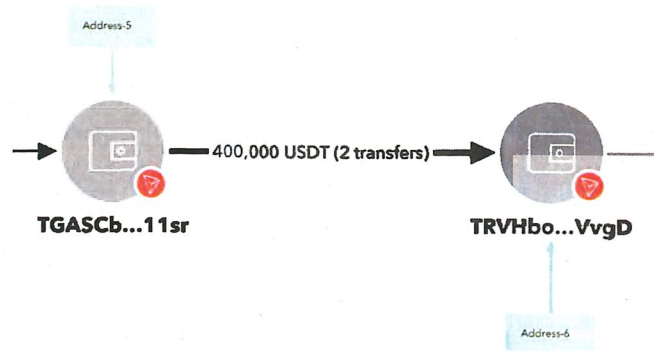


involved in the transfer of victim funds in other reported fraud schemes. Although none of the funds from L.D. (J.K.'s sister) ended up in **ADDRESS-8**, funds from L.D. were traced to account holders at OKX and some were transferred to ADDRESS-4 as well.

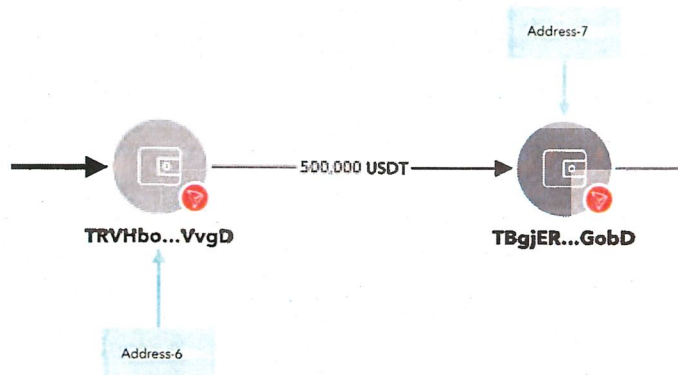
45. One hour after the funds were received in ADDRESS-4 - still on June 5, 2024 - approximately 198,950 USDT (\$198,950) was transferred to the address beginning/ending TGASCb . . . 11sr (ADDRESS-5). Using the Proceeds In, First Out tracing methodology, the 198,950 USDT transferred were all funds that belonged to J.K.



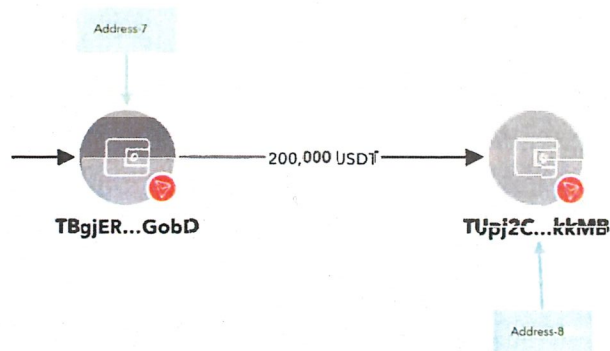
46. Less than three hours after the funds were received in ADDRESS-5, the next two transfers out were made to the address beginning/ending TRVHbo . . . VvgD (ADDRESS-6). The first transfer out was for approximately 10,000 USDT (\$10,000). Using the Proceeds In, First Out tracing methodology, this transfer consisted entirely of funds belonging to J.K. Two minutes after the first transfer, a larger transfer of approximately 390,000 USDT was made to ADDRESS-6. Using the Proceeds In, First Out tracing methodology, this transfer consisted of 188,950 USDT (\$188,950) of funds belonging to J.K.:



47. The funds then remained in ADDRESS-6 until August 21, 2024, when they were moved as part of a larger transfer of 500,000 USDT to the address beginning/ending TBgjER . . . GobD (ADDRESS-7). Using the Proceeds In, First Out tracing methodology, this transfer included the approximately 198,950 USDT (\$198,950) of funds belonging to J.K.



48. Less than two minutes after being received in ADDRESS-7, a transfer of 200,000 USDT was made to the address beginning/ending TUpj2C . . . kkMB (ADDRESS-8). Using the Proceeds In, First Out tracing methodology, this transfer included the 198,950 USDT (\$198,950) of funds belonging to J.K. Also, at the time of the transfer, ADDRESS-8 had a preexisting balance of approximately 125,060 USDT.



49. On December 31, 2024, the USDT in **ADDRESS-8** was frozen by Tether Limited, Inc. At the time of the freeze, **ADDRESS-8** had a balance of approximately 325,060 USDT (\$325,060), which was the same 325,060 USDT that was in **ADDRESS-8** following the August 21, 2024, transfer described above.

50. Pursuant to a federal seizure warrant issued by U.S. Magistrate Judge Carmen E. Henderson on March 20, 2025, Tether Limited, Inc., “burned” the USDT tokens associated with **ADDRESS-8** and reissued the equivalent amount of USDT tokens [namely, 325,060 USDT] to a U.S. law enforcement-controlled virtual currency wallet.

51. The identity of the owner(s) of **ADDRESS-8** is unknown. The only available information to law enforcement is the cryptocurrency address itself. Notice of this action will be messaged via the Tron blockchain to the address with a link to a copy of this Complaint in Forfeiture.

VIII. *CONCLUSION: FORFEITURE OF ALL TETHER (USDT) CRYPTOCURRENCY (NAMELY, 325,060 USDT VALUED AT APPROXIMATELY \$325,060) FORMERLY HELD AT ADDRESS-8.*

52. Based upon the foregoing, the defendant 325,060 USDT (\$325,060) constitutes, or is derived from, proceeds traceable to wire fraud/wire fraud conspiracy and, further, was



involved in a transaction(s) in violation of 18 U.S.C. § 1956(a)(1)(B)(i) (concealment money laundering), or is property traceable to such property.

53. Particularly, all funds formerly held at **ADDRESS-8** (325,060 USDT) are proceeds of wire fraud/conspiracy to commit wire fraud and, accordingly, are subject to forfeiture under 18 U.S.C. § 981(a)(1)(C). In addition to the funds stolen from J.K. contained in **ADDRESS-8** - namely, the 198,950 USDT (\$198,950) - the other USDT in **ADDRESS-8** bears the hallmarks of proceeds of cryptocurrency fraud schemes. In total, five deposits of USDT were made into **ADDRESS-8** and there were no withdrawals made. At the time of the transfer of J.K.'s funds, **ADDRESS-8** had a preexisting balance of approximately 125,060 USDT. Of this 125,060 USDT, approximately 68,969 USDT (\$68,969) was transferred in directly from **ADDRESS-4** via **ADDRESS-3**. As set forth above, **ADDRESS-4** is known to be used as a transit address for stolen funds from multiple different victims of cryptocurrency fraud schemes. The remaining three transfers totaled \$56,091, all coming from an unhosted wallet address which is known by investigators to have had direct transfers from OKX and indirect transfers from **ADDRESS-4**.

54. The transfer of the 200,000 USDT on August 21, 2024, from **ADDRESS-7** into **ADDRESS-8** - of which 198,950 USDT belonged to J.K. - constituted a money laundering transaction in violation of 18 U.S.C. § 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 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/or control of the SUA proceeds.

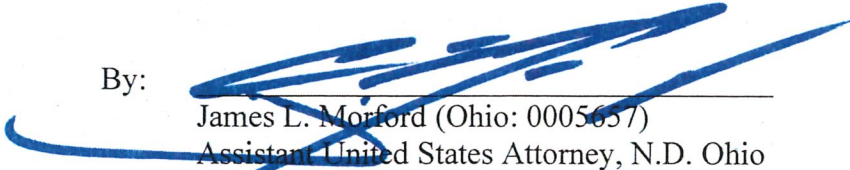
55. Under 18 U.S.C. § 981(a)(1)(A), all property - real and personal - “involved in” or traceable to an offense in violation of § 1956(a)(1)(B)(i) is subject to forfeiture. In this regard, “other funds” in a cryptocurrency address into which SUA proceeds are transferred as part of a concealment money laundering offense (*i.e.*, the preexisting balance of approximately 125,060 USDT in **ADDRESS-8**) - along with the SUA proceeds and 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. “Other funds” commingled with the SUA proceeds obfuscate the origin or existence of the SUA proceeds. Therefore, all funds in **ADDRESS-8** were “involved in” concealment money laundering and are subject to forfeiture under 18 U.S.C. § 981(a)(1)(A).

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,

David M. Toepfer  
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<sup>th</sup> day of August, 2025.

  
Notary Public



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