

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

UNITED STATES OF AMERICA,)	CASE NO.
)	
Plaintiff,)	
)	JUDGE
v.)	
)	
100,000 TETHER (“USDT”))	
CRYPTOCURRENCY, VALUED AT)	
APPROXIMATELY \$100,000.00, FORMERLY)	
ASSOCIATED WITH CRYPTOCURRENCY)	
ADDRESS ENDING 35345a3, and)	
)	
100,000 TETHER (“USDT”))	
CRYPTOCURRENCY, VALUED AT)	
APPROXIMATELY \$100,000.00, FORMERLY)	
ASSOCIATED WITH CRYPTOCURRENCY)	
ADDRESS ENDING 700f10e,)	
)	
Defendants.)	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 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).

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 now 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” - 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.

II. *DESCRIPTION OF THE DEFENDANT PROPERTIES*

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

a.) 100,000 Tether (“USDT”) cryptocurrency, valued at approximately \$100,000.00, formerly associated with the cryptocurrency address beginning/ending 0xa51 . . . 35345a3 on the

Ethereum blockchain. On or about March 19, 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 Jennifer D. Armstrong on July 31, 2024, Tether Limited “burned” the USDT tokens then associated with the cryptocurrency address and reissued the equivalent amount of USDT tokens [namely, 100,000 USDT] to a U.S. law enforcement-controlled virtual currency wallet. The cryptocurrency address beginning/ending 0xa51 . . . 35345a3 is referred to in the following paragraphs as “**ADDRESS-7**”.

b.) 100,000 Tether (“USDT”) cryptocurrency, valued at approximately \$100,000.00, formerly associated with the cryptocurrency address beginning/ending 0x7c1 . . . 700f10e on the Ethereum blockchain. On or about March 19, 2024, the USDT tokens at the cryptocurrency address were frozen by 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 then associated with the cryptocurrency address and reissued the equivalent amount of USDT tokens [namely, 100,000 USDT] to a U.S. law enforcement-controlled virtual currency wallet. The cryptocurrency address beginning/ending 0x7c1 . . . 700f10e is referred to in the following paragraphs as “**ADDRESS-8**”.

7. The identity of the owner(s) of the cryptocurrency addresses described above is 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 the Complaint in Forfeiture.

III. *STATUTES*

8. This Complaint in Forfeiture relates to violations of 18 U.S.C. Section 1343 (wire fraud) and conspiracy to commit the offense in violation of 18 U.S.C. Section 371 (wire fraud

conspiracy). Title 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.

9. The term “specified unlawful activity” is defined in 18 U.S.C. Sections 1956(c)(7) and 1961(1), and it includes violations of 18 U.S.C. Section 1343 (wire fraud).

10. 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, or a conspiracy to commit such offense, is subject to civil forfeiture.

IV. *BACKGROUND ON CRYPTOCURRENCY*

11. *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.

12. *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.

13. *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.

14. *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.

15. *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 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.

16. *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.

17. *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).

18. *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.

19. *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 and 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.

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

V. *BACKGROUND OF INVESTIGATION*

21. The Federal Bureau of Investigation (FBI), Cleveland Field Office, is investigating cryptocurrency confidence fraud scams perpetrated on victims throughout the United States, including in the Northern District of Ohio.

22. On or about February 22, 2024, a victim in Ashtabula, Ohio, with the initials “L.D.” filed a complaint with the FBI’s Internet Crime Complaint Center reporting losses from a

scam. The incident began when L.D. attempted to transfer bitcoin (“BTC”) he owned off of his Trezor hardware wallet onto a website called ThorSwap using the “earn” feature. Doing so would have enabled L.D. to earn interest on his BTC by allowing the ThorSwap website to use it in liquidity pools, keeping some of the interest earned for itself and providing some back to L.D. Essentially, L.D. would be lending ThorSwap his BTC to use in crypto-based financial transactions and would be earning a defined interest rate for doing so.

23. L.D. learned how to do this by watching YouTube promoters discuss how to earn interest on BTC using ThorSwap.

24. Following the instructions on what he believed to be the legitimate website for ThorSwap, L.D. connected his Trezor wallet to the website and went through the steps to authorize a transfer of 1 BTC (\$50,000.00) on or about February 20, 2024. That transaction was processed on or about February 20, 2024, and is recorded on the BTC blockchain.

25. The transfer of 1 BTC, however, did not end up in a wallet belonging to ThorSwap. A transfer to a wallet controlled by ThorSwap for the “earn” feature would contain the phrase “BTC.BTC” in the OP RETURN field as part of the information available for each BTC blockchain transaction. The transfer initiated by L.D. had an OP RETURN field that was blank, and the wallet that received the 1 BTC is not known to be associated with ThorSwap.

26. L.D. advised law enforcement that had the 1 BTC transaction to ThorSwap been successful, he would have been willing to transfer an additional two or three BTC to the site, but not the full remainder of his BTC holdings on the Trezor wallet.

27. Upon realizing that he had lost 1 BTC to an unknown address - as BTC transactions are irreversible - L.D. then began reaching out to remedy the issue. He contacted SatoshiLabs, the company that manufactures and sells Trezor hardware wallets. He also

contacted ThorSwap using the features available on the site. He additionally sought assistance on X (formerly Twitter) and Discord to get advice on how to try and recover the 1 BTC that was no longer on his wallet nor with ThorSwap.

28. Two days after this incident, on or about February 22, 2024, a fraudulent transfer of the remaining 6.55813405 BTC (\$340,000.00) was made from L.D.'s Trezor wallet to the cryptocurrency address beginning/ending 1Bb2g . . . NcxT, an address unknown to L.D. L.D. did not initiate or authorize the transaction.

29. The cryptocurrency address beginning/ending 1Bb2g . . . NcxT is referred to in the following paragraphs as "**ADDRESS-1**".

30. L.D. did not purchase the Trezor hardware wallet directly from the company. He purchased it from a re-seller on Amazon.com.

31. L.D. would not have sent the full 6.55813405 BTC to any unknown party and, further, would not have sent the funds to unknown actors accessing computers from Nigeria.

VI. TRACING ANALYSIS

32. As set forth in paragraph 28, on or about February 22, 2024, 6.55813405 BTC (\$340,000.00) was moved from L.D.'s wallet to the unhosted wallet address beginning/ending 1Bb2g . . . NcxT (**ADDRESS-1**). At the time of this transfer into **ADDRESS-1**, there was no other BTC contained in **ADDRESS-1**, and this represented the first transaction involving **ADDRESS-1**.

33. On or about February 22, 2024, the entire balance of 6.55813405 BTC was transferred from **ADDRESS-1** - in five different transactions - to addresses controlled by the MEXC Global Limited cryptocurrency exchange as follows:

- a.) 1 BTC (\$50,000.00) to the cryptocurrency address beginning/ending 3BLdS . . . y6GX (**ADDRESS-2**) at approximately 6:26 p.m. Eastern Time.
- b.) 0.5 BTC (\$25,000.00) to the cryptocurrency address beginning/ending 3P3RN . . . vwyq (**ADDRESS-3**) at approximately 7:21 p.m. Eastern Time.
- c.) 1 BTC (\$50,000.00) to the cryptocurrency address beginning/ending 3BLdS . . . y6GX (**ADDRESS-2**) at approximately 7:43 p.m. Eastern Time.
- d.) 2 BTC (\$100,000.00) to the cryptocurrency address beginning/ending 33n7g . . . NBUr (**ADDRESS-4**) at approximately 7:48 p.m. Eastern Time.
- e.) 2.05785045 BTC (\$100,000.00) to the cryptocurrency address beginning/ending 38RWF . . . n5AG (**ADDRESS-5**) at approximately 8:33 p.m. Eastern Time.

34. On or about February 22, 2024, an account at the MEXC Global Limited cryptocurrency exchange - with control over **ADDRESS-2** and registered with the e-mail address ending inbig@gmail.com - swapped 1 BTC for approximately 51,371 USDT (\$51,371.00). Before this swap, the account ofbig@gmail.com had a balance of zero USDT and 1 BTC, which represented the transfer detailed in paragraph 33(a). At approximately 7:29 p.m. Eastern Time on or about February 22, 2024, the 51,371 USDT was transferred from thebig@gmail.com account to the unhosted wallet address beginning/ending 0x7e0 . . . b110 (**ADDRESS-6**). The user initiating these transactions on MEXC Global Limited was logged into an Apple Device using iOS software.

35. Thebig@gmail.com account at MEXC Global Limited was created on or about February 18, 2024. Thebig@gmail.com address was created with Google on or about February 18, 2024.

36. Thebig@gmail.com address was accessed on or about February 22, 2024, from an iPhone running iOS software from an IP address of xxx.xx.58.173. That IP address geolocates to Lagos, Nigeria, under the control of MTN Nigeria Communication Limited.

37. On or about February 22, 2024, an account at the MEXC Global Limited cryptocurrency exchange - with control over **ADDRESS-3** and identified only with the number SFP5557xxxxxxx - swapped 0.5 BTC (\$25,000.00) for approximately 8.560342 Ethereum (ETH). Before this swap, the account of SFP5557xxxxxxx had a balance of zero ETH and 0.5 BTC, which represented the transfer detailed in paragraph 33(b). At approximately 7:59 p.m. Eastern Time on or about February 22, 2024, the 8.560342 ETH was transferred from the SFP5557xxxxxxx account to **ADDRESS-6**.

38. On or about February 22, 2024, thebig@gmail.com account at the MEXC Global Limited cryptocurrency exchange swapped 1 BTC for approximately 51,452 USDT (\$51,452.00). Before this swap, the account ofbig@gmail.com had a balance of zero USDT and 1 BTC, which represented the transfer detailed in paragraph 33(c). At approximately 7:56 p.m. Eastern Time on or about February 22, 2024, the 51,452 USDT was transferred from thebig@gmail.com account to **ADDRESS-6**. The user initiating these transactions on MEXC Global Limited was logged into an Apple Device using iOS software.

39. On or about February 22, 2024, an account at the MEXC Global Limited cryptocurrency exchange - with control over **ADDRESS-4** and registered with the e-mail address ending inwaters@gmail.com - swapped 2 BTC for 102,925 USDT (\$102,925.00). Before this swap, the account ofwaters@gmail.com had a balance of zero USDT and 2 BTC, which represented the transfer detailed in paragraph 33(d). At approximately 8:07 p.m. Eastern Time on or about February 22, 2024, the 102,925 USDT was transferred from thewaters@gmail.com account to **ADDRESS-6**. The user initiating these transactions on MEXC Global Limited was logged into an Apple Device using iOS software.

40. Thewaters@gmail.com account at MEXC Global Limited was created on or about February 22, 2024. Thewaters@gmail.com address was created with Google on or about February 22, 2024, and then deleted on or about February 23, 2024.

41. Thewaters@gmail.com account was accessed multiple times on or about February 22, 2024, from the IP address xxx.xxx.109.51. That IP address geolocates to Lagos, Nigeria, under the control of Airtel Networks Limited. Thewaters@gmail.com account was accessed once on or about February 22, 2024, using a VPN service with an iPhone running iOS software.

42. **ADDRESS-6** had a zero balance of either ETH or USDT at the time it received transactions of USDT and ETH from thebig@gmail.com, SFP5557xxxxxxx, andwaters@gmail.com accounts at the MEXC Global Limited cryptocurrency exchange. Those transfers represented the first transactions on the blockchain involving **ADDRESS-6**.

43. As cryptocurrency transactions are irreversible, address owners will often send a “test transaction” of a smaller amount to an address to ensure that it goes through before sending a larger amount to the same address.

44. On or about February 22, 2024, at approximately 10:12 p.m. Eastern Time, a test transaction of 2,000 USDT (\$2,000.00) was sent from **ADDRESS-6** to the subject cryptocurrency address beginning/ending 0xa51 . . . 35345a3 (**ADDRESS-7**). On or about February 22, 2024, at approximately 10:13 p.m. Eastern Time, a transaction of 98,000 USDT (\$98,000.00) was sent from **ADDRESS-6** to the subject **ADDRESS-7**. At the time of the transfers, **ADDRESS-7** had a balance of zero USDT and the two transfers represent the only activity involving **ADDRESS-7** on the blockchain.

45. On or about March 19, 2024, the USDT tokens at **ADDRESS-7** were frozen by Tether Limited.

46. Approximately \$100,000.00 of the funds that were fraudulently transferred out of L.D.'s wallet on or about February 22, 2024, are traceable to **ADDRESS-7**.

47. On or about February 23, 2024, at approximately 8:16 a.m. Eastern Time, a transaction of 100,000 USDT (\$100,000.00) was sent from **ADDRESS-6** to the subject cryptocurrency address beginning/ending 0x7c1 . . . 700f10e (**ADDRESS-8**). At the time of the transfer, **ADDRESS-8** had a balance of zero USDT and this single transfer represents the only activity involving **ADDRESS-8** on the blockchain.

48. On or about March 19, 2024, the USDT tokens at **ADDRESS-8** were frozen by Tether Limited.

49. Approximately \$100,000.00 of the funds that were fraudulently transferred out of L.D.'s wallet on or about February 22, 2024, are traceable to **ADDRESS-8**.

VII. *CONCLUSION*

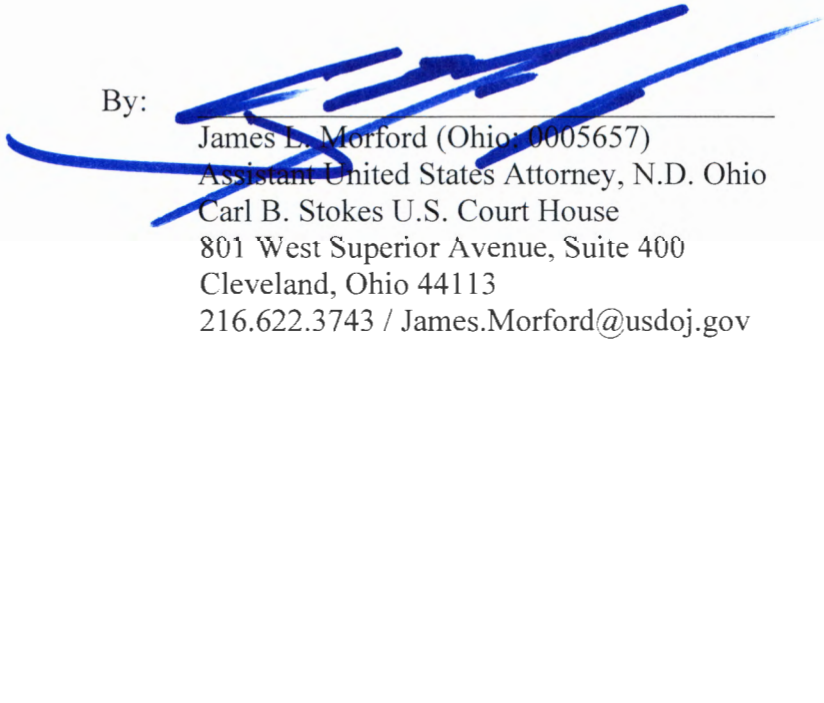
50. By reason of the foregoing, the defendant properties [namely: (i) 100,000 Tether ("USDT") cryptocurrency, valued at approximately \$100,000.00, formerly associated with the cryptocurrency address beginning/ending 0xa51 . . . 35345a3; and, (ii) 100,000 Tether ("USDT") cryptocurrency, valued at approximately \$100,000.00, formerly associated with the cryptocurrency address beginning/ending 0x7c1 . . . 700f10e] are subject to forfeiture to the United States under 18 U.S.C. Section 981(a)(1)(C) in that they constitute - or are derived from - proceeds traceable to violation(s) of 18 U.S.C. Section 1343 (wire fraud) and 18 U.S.C. Section 371 (conspiracy to commit wire fraud).

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 according to 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:

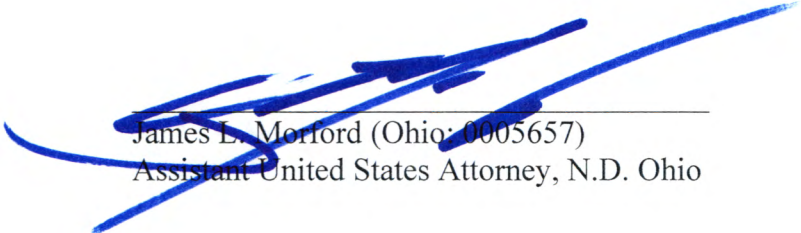


James L. Morford (Ohio: 0005657)
Assistant United States Attorney, N.D. Ohio
Carl B. Stokes U.S. Court House
801 West Superior Avenue, Suite 400
Cleveland, Ohio 44113
216.622.3743 / James.Morford@usdoj.gov

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 2nd day of October, 2024.


Notary Public



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