UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

vs. No. 1:25-cv-1660

10,000 Tether (USDT) from address ending 1A14 (Subject Address 1),

40,844.2101170 Tether (USDT) from address ending 1880 (Subject Address 2),

6,000 Tether (USDT) from address ending 5B27 (Subject Address 3), and

1,119,684.148652 Tether (USDT) from address ending C970 (Subject Address 4),

Defendant Property.
_____/

VERIFIED COMPLAINT FOR FORFEITURE IN REM

NOW COMES Plaintiff, United States of America, by and through its attorneys, Timothy P. Verhey, United States Attorney for the Western District of Michigan, and Daniel T. McGraw, Assistant United States Attorney, and states upon in formation and belief that:

NATURE OF ACTION

1. This is a civil forfeiture action filed pursuant to 18 U.S.C. §§ 981(a)(1)(A), 981(a)(1)(C) and Supplemental Rule G(2) of the Federal Rules of Civil Procedure to forfeit and condemn to the use and benefit of the United States of America the following property:

a. 10,000 Tether (USDT) from virtual currency address ending 1A14 (Subject Address 1);

b. 40,844.2101170 Tether (USDT) from virtual currency address ending 1880 (Subject Address 2);

c. 6,000 Tether (USDT) from virtual currency address ending 5B27 (Subject Address 3); and

d. 1,119,684.148652 Tether (USDT) from virtual currency address ending C970 (Subject Address 4),

collectively, approximately 1,176,528.36 Tether USDT from the Subject Addresses (the "Defendant Property").

THE DEFENDANT IN REM

2. The Defendant Property consists of

a. 10,000 Tether (USDT) from virtual currency address ending 1A14 (Subject Address 1);

b. 40,844.2101170 Tether (USDT) from virtual currency address ending 1880 (Subject Address 2);

c. 6,000 Tether (USDT) from virtual currency address ending 5B27 (Subject Address 3); and

d. 1,119,684.148652 Tether (USDT) from virtual currency address ending C970 (Subject Address 4),

collectively, approximately 1,176,528.36 Tether USDT from the Subject Addresses, that was seized on or about July 17, 2025 by the Federal Bureau of Investigation ("FBI") pursuant to a seizure warrant authorized by the United States District Court for the Western District of Michigan. The Defendant Property is currently in the custody of the United States Marshals Service ("USMS").

JURISDICTION AND VENUE

3. This Court has jurisdiction over this proceeding pursuant to 28 U.S.C. §§ 1345 and 1355(b)(1)(A), because this action is being commenced by the United States of America as Plaintiff, and the acts giving rise to the basis for forfeiture occurred in this judicial district.

4. Venue is proper before this Court pursuant to 28 U.S.C. § 1355(b)(1) because the acts or omissions giving rise to forfeiture occurred in this judicial district, and/or pursuant to 28 U.S.C. § 1395(b), because the Defendant Property was found within this judicial district.

BASIS FOR FORFEITURE

5. As set forth below, the Defendant Property is subject to civil forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(A) because it is any property, real or personal, involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956(a)(1)(B)(i), or any property traceable to such property; and pursuant to 18 U.S.C. § 981(a)(1)(C) because it is any property, real or personal, which constitutes or is derived from proceeds traceable to wire fraud, in violation of 18 U.S.C. § 1343.

6. Under 18 U.S.C. § 1956(a)(1)(B)(i), it is a criminal offense for anyone, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conducts such 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 the specified unlawful activity, here, wire fraud, in violation of 18 U.S.C. § 1343.

7. Under 18 U.S.C. § 1343, it is a criminal offense for anyone who has devised a scheme or artifice to defraud, or anyone who has devised a scheme or artifice to obtain money by means of false or fraudulent pretenses, representations, or promises, to transmit by means of wire, radio, or television communication in interstate commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing the scheme or artifice.

8. Under 18 U.S.C. § 1956(h), it is a criminal offense to conspire to commit any offense described in section 1956, including 1956(a)(1)(B)(i).

FACTS SUPPORTING FORFEITURE

Background on Cryptocurrency

9. Virtual currencies are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank, like traditional fiat currencies such as the U.S. dollar, but are generated and controlled through computer software. Bitcoin is the most well-known virtual currency in use.

10. 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 alphanumeric characters. Each virtual currency address is controlled through a unique corresponding private key—the equivalent of a passworded needed to access the address. Only the hold of

an address's private key can authorize a transfer of virtual currency from that address to another address.

11. Many virtual currencies publicly record their transactions on what is referred to and known as the "blockchain." The blockchain is essentially a distributed public ledger, run by a decentralized network, containing an immutable record of every transaction that has ever occurred using that blockchain's specific technology. The blockchain can be updated multiple times per hour and records every virtual currency address that ever received that virtual currency. It also 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.

12. Although the identity of an address owner is generally anonymous (unless the owner opts to make the information publicly available), analysis of the blockchain can often be used to identify the owner of a particular address. The analysis can also, in some instances, reveal additional addresses controlled by the same user. A user of virtual currency can operate multiple addresses at any given time and there is no limit to the number of addresses any user can have.

13. A virtual currency 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 also allows users to send and receive virtual currencies. Multiple addresses can be stored in a single wallet.

Background on Stablecoins

14. Stablecoins are a type of virtual currency whose value is pegged to a commodity's prices, such as gold, or to a fiat currency, such as the U.S. dollar, or to a different virtual currency. For example, USDT is a stablecoin pegged to the U.S. dollar. Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives.

Background on Tether Limited

15. Tether Limited is a company that manages the smart contracts and the treasury (*i.e.*, the funds held in reserve) for USDT. The value of USDT is tied to the value of the U.S. dollar. According to Tether Limited, one USDT is backed by one U.S. dollar held in Tether Limited's reserves. For this reason, USDT is known as a "stablecoin"—a term used to describe a virtual currency that has a value pegged to a fiat currency or the value of a commodity. USDT is hosted on the Ethereum (ETH) and Tron blockchains, among others.

Cryptocurrency Investment Fraud Scheme

16. On April 14, 2025, the FBI received on online tip from an employee at Charlevoix State Bank (CSB) in Boyne City, Michigan, within the Western District of Michigan, that reported suspected fraudulent transactions associated with Victim 1's financial accounts.

17. According to CSB, Victim 1 had recently received multiple incoming wire transfers from numerous individuals and subsequently initiated outgoing wire transfers to Coinbase, a well-known cryptocurrency exchange.[1]

18. An analysis of Victim 1's accounts at CSB revealed that between February 27, 2025 and April 17, 2025, Victim 1 received approximately $1,284,000 in wire transfers, and initiated outgoing wire transfers totaling approximately $1,282,000. Specifically, on April 10, 2025, two wire transfers totaling $400,000 were received into Victim 1's account from a Chase bank account registered to another individual, Victim 2.

19. On April 23, 2025, Victim 2, a resident of Arizona, submitted a complaint to the FBI Internet Crime Complaint Center stating that they had been victimized by an investment fraud scheme. Victim 2 reported that they wired a total of $620,000 to three different bank accounts under the false pretense that it would be legitimately invested into cryptocurrency. Two of the outgoing wires by Victim 2 totaling $400,000 were sent to Victim 1's CSB account in the Western District of Michigan on April 10, 2025.

20. An additional analysis of Victim 1's CSB account revealed that on April 17, 2025, Victim 1 initiated a wire transfer to Coinbase in the amount of $400,000.

21. On July 7, 2025, FBI agents interviewed Victim 1 in Boyne City, Michigan. During the interview, Victim 1 stated that they believed all wire transfers

[1] Coinbase Global, Inc. ("Coinbase") is an American cryptocurrency exchange. According to its public website, Coinbase is available in over 100 countries and has $328 billion assets on its platform.

Victim 1 sent between February 27, 2025 and April 17, 2025 were for a legitimate cryptocurrency investment opportunity presented to Victim 1 by an unidentified online romantic partner ("the Subject"). The Subject led Victim 1 to believe they wanted to be in an exclusive romantic relationship. Upon gaining Victim 1's confidence, the Subject presented a cryptocurrency investment opportunity with promises of high returns. Once the Subject learned that Victim 1 only had $5,000.00 to invest, the Subject, under false pretenses, provided instructions to receive incoming wire transfers from "business partners" who allegedly owed the Subject money. The Subject then provided Victim 1 a series of instructions to wire the money to a well-known legitimate cryptocurrency exchange, swap the fiat currency for virtual currency, and ultimately invest the funds into a fraudulent cryptocurrency trading platform. Ultimately, Victim 1 transferred approximately $1,300,000 under false pretenses.

22. Specifically, according to Victim 1, and a review Victim 1's CSB account records and Victim 1's Coinbase account records, between February 27, 2027 and April 17, 2025, Victim 1 transferred approximately $1,287,533.20 of USDC[2] out of Victim 1's Coinbase account to two specific, identified virtual currency addresses.

[2] USDC is a stablecoin pegged to the U.S. dollar. Circle Internet Financial, LLC ("Circle") is a cryptocurrency exchange. Circle manages the smart contracts and treasury for USDC.

From these transfers, ultimately, approximately $1,252,000 of the value was converted to USDT utilizing the decentralized exchange Uniswap.[3]

23. Upon information and belief, decentralized exchanges are virtual currency trading platforms or marketplaces that operate directly between virtual currency traders, without an intermediary or centralized exchange. Utilizing decentralized exchanges to convert from one type of virtual currency to another type of virtual currency is a common technique used to obfuscate the origination and destination of virtual currency assets. Converting one type of virtual currency for another is commonly known as "swapping."

24. In the swaps from USDC to USDT discussed above, the value of the USDT was broken down amongst the following virtual currency addresses:

Address	Approximate USD Value
0x489BEF11045822CF9C97F9FA1968D8d48203a851	$399,861.65
0xE9e537316Ed2d6b839F1e3d477f0645866D74f3c	$369,971.44
0x3E2356CcA26E78aa84de5c6a126D3565dC9A5EFE	$482,922.66

25. According to an FBI tracing analysis, on April 9, 2025, 200,000 USDT was transferred from the address ending "D74f3c" and deposited into an address ending "03a851." On April 10, 2025, "03a851" sent 40,000 USDT to Subject Address 1. As of July 14, 2025, according to the public Ethereum blockchain, Subject Address 1 had no other deposits and maintained a current balance of 10,000 USDT.

[3] According to its publicly available website, "Uniswap products are powered by the Uniswap Protocol. The protocol is the largest onchain marketplace, with billions of dollars in weekly volume across thousands of tokens on Ethereum and 12+ additional chains."

26. Between April 23, 2025 and June 9, 2025, the address ending "03a851" sent 66,013 USDT to Subject Address 2. As of July 14, 2025, according to the public Ethereum blockchain, Subject Address 2 had no other deposits over $1 in value and maintained a current balance of 40,844 USDT.

27. On April 30, 2025, Subject Address 2 sent 6,000 USDT to Subject Address 3. As of July 14, 2025, according to the public Ethereum blockchain, Subject Address 3 had no other deposits or withdrawals and maintained a current balance of 6,000 USDT.

28. FBI completed additional tracing analysis on the address ending "03a851." On April 19, 2025, at 16:37 UTC, 200,000 USDT was transferred to an address sending "06C8E5." On April 20, 2026, at 06:11 UTC and 06:14 UTC, two transfers totaling 200,000 USDT were sent from the address ending "06C8E5" to Subject Address 4. Within ten minutes of the deposit into Subject Address 4, the 200,000 USDT was comingled with an additional 190,000 USDT and sent to an address ending "725C7f." The 390,000 USDT was all swapped from USDT to ETH[4] and comingled with an additional 310,000 USDT that was swapped to ETH. The additional 310,000 USDT was deposited into "725C7f" less than a half hour after the deposit from Subject Address 4 and was transferred in from the same address ending "06C8E5." On April 20, 2025, by 06:50 UTC, all 700,000 USDT that were swapped to ETH (minus transaction fees) were redeposited back into Subject Address 4 as ETH.

[4] ETH, or Ether, is the native virtual currency for the Ethereum blockchain.

29. Subject Address 4 had no additional transactions until May 14, 2025. On May 14, 2025, between 10:11 UTC and 12:49 UTC, ETH was swapped for USDT totaling 1,119,684.15 USDT. As of July 14, 2025, according to the public Ethereum blockchain, Subject Address 4 had no additional deposits or withdrawals and maintained a current balance of 1,119,684.148652 USDT.

30. In summary, according to the public Ethereum blockchain, as of July 14, 2025, there as 1,176,528.36 USDT in the Subject Addresses, the Defendant Property. On July 17, 2025, pursuant to a seizure warrant, the FBI seized the Defendant Property.

31. Upon information and belief, the Defendant Property constitutes proceeds of wire fraud, and property involved in money laundering, all of which is subject to forfeiture to the United States.

32. Upon information and belief, the Subject Addresses were used to commit, and therefore involved in, concealment money laundering. Criminals often conduct an otherwise unnecessary and costly number of transactions to transfer criminal proceeds via layered transactions designed to conceal or disguise the nature, location, source, ownership, or control of those proceeds. The large number of rapid transfers described above—which have no apparent legitimate purpose—strongly indicate that these funds were transacted in a way designed to conceal or disguise the nature, location, source, ownership, or control of the proceeds of a specified unlawful activity, in this case, wire fraud.

33. The public Ethereum blockchain analysis in this case, summarized above, demonstrates that the proceeds of the wire fraud scheme were broken up, distributed through a series of cryptocurrency virtual addresses via rapid transactions, and re-consolidated with other funds in the Subject Addresses.

34. The commission of convoluted, intermingled, and re-consolidated transactions, which incurred transaction fees and served no apparent legitimate purpose, imply that the "purpose of these numerous, fast-repeating, and intermingled transactions was to conceal the nature, source, location, ownership and control of the proceeds." *See, e.g.*, *United States v. Sterlingov*, No. 1:21-cr-00399-RDM, 2023 WL 2387759, *7 (D.D.C. Mar. 6, 2023) (concluding that "there is probable cause to believe that [defendant's] seized funds"—even if not proceeds of crime—"were 'involved in'" defendant's Bitcoin tumbler business' "unlicensed money transmitting operations" that mixed Bitcoins for a fee, making it more difficult to trace); *United States v. Rodriguez*, 53 F.3d 1439, 1447-48 (7th Cir. 1995) (convoluted real estate transactions, from which intent to conceal or disguise may be inferred, also imply knowledge of illegal source; jury could infer knowledge from combination of suspicion and indifference to the truth).

35. Where it is shown that a suspected money launderer commingled proceeds of specified unlawful activity with untraced funds in an address or wallet via such transactions apparently designed to conceal the nature, source, ownership, location, or control of criminal proceeds, then those commingled untraced funds are forfeitable as having facilitated—and therefore as having been "involved in"—

concealment money laundering. *See, e.g.*, *United States v. Bikundi*, 926 F.3d 761, 793-94 (D.C. Cir. 2019) (collecting cases); *see also United States v. Guerrero*, 2021 WL 2550154, *9 (N.D. Ill June 22, 2021) (money from unknown source that was commingled with fraud proceeds facilitated the concealment laundering of fraud proceeds and, accordingly, property acquired with the commingled funds was forfeitable as property traceable to property involved in a money laundering offense); *United States v. Romano*, 2021 WL 1711633, *5-6 (E.D.N.Y. Apr. 29, 2021) (by laundering fraud proceeds through their personal bank accounts, to commingle the proceeds with other funds for a concealment laundering purpose, the defendants made the commingled funds forfeitable as facilitating property); *United States v. Coffman*, 859 F. Supp. 2d 871, 876-77 (E.D. Ky. 2012) (holding that forfeiture of legitimate and criminal proceeds commingled in an account is proper as long as the government demonstrates that the defendant pooled the funds to facilitate money laundering by, for example, disguising the nature and source of proceeds; concluding that clean funds in bank account were subject to forfeiture because they had "been co[m]mingled with tainted funds for the purpose of obfuscating the origin or existence of tainted money.").

36. The transfer of fraud proceeds from multiple victims into the same address or financial account via transactions committed within a relatively short time period strongly indicates that the other funds contained in the address or account are also fraud proceeds and, likewise, that the address or account is being used to collect,

conceal, and launder those funds. As shown above, this matter involves such transfers of criminal proceeds into the Subject Addresses.

CLAIM I

37. Plaintiff hereby re-alleges paragraphs 1 – 36, as referenced above.

38. The Defendant Property is forfeitable to the United States pursuant to 18 U.S.C. § 981(a)(1)(A) because it is any property, real or personal, involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956 or any property traceable to such property.

CLAIM II

39. Plaintiff hereby re-alleges paragraphs 1 – 36, as referenced above.

40. The Defendant Property is forfeitable to the United States pursuant to 18 U.S.C. § 981(a)(1)(C) because it is any property, real or personal, which constitutes or is derived from proceeds traceable to wire fraud, in violation of 18 U.S.C. § 1343.

REQUESTED RELIEF

Wherefore, the United States requests that the Court issue a warrant for the arrest of the Defendant Property; that due notice be given to all interested parties to appear and show cause why forfeiture to the United States of America should not be decreed; and that the Defendant Property be condemned and forfeited to the United States of America and be delivered into the custody of the United States Marshals Service for disposition according to law; and for such other relief as this Court may deem just and proper.

TIMOTHY VERHEY
United States Attorney

Dated: December 5, 2025

DANIEL T. McGRAW
Assistant United States Attorney
P.O. Box 208
Grand Rapids, Michigan 49501-0208
(616) 456-2404

VERIFICATION

I am a Special Agent with the Federal Bureau of Investigation with personal involvement in this investigation.

I have read the contents of the foregoing Verified Complaint for Forfeiture In Rem, and the statements contained therein are true to the best of my knowledge and belief.

I declare under penalty of perjury that the foregoing is true and correct.

Dated: 12/04/2025

JUSTIN R HALL
Special Agent
Federal Bureau of Investigation