IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF OHIO

EASTERN DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. 4,340,000 TETHER ("USDT") CRYPTOCURRENCY, VALUED AT APPROXIMATELY $4,340,000, FORMERLY ASSOCIATED WITH CRYPTOCURRENCY ADDRESS BEGINNING/ENDING 0xa17 . . . 44f0021, 3,290,000 TETHER ("USDT") CRYPTOCURRENCY, VALUED AT APPROXIMATELY $3,290,000, FORMERLY ASSOCIATED WITH CRYPTOCURRENCY ADDRESS BEGINNING/ENDING 0x4e5 . . . d47abb5, and 577,578 TETHER ("USDT") CRYPTOCURRENCY, VALUED AT APPROXIMATELY $577,578, FORMERLY ASSOCIATED WITH CRYPTOCURRENCY ADDRESS BEGINNING/ENDING 0xafd . . . b2378a5, Defendants.	)	CASE NO. 1:25-CV-386 JUDGE SOLOMON OLIVER, JR. **FINAL ORDER OF FORFEITURE**

This is an action for the civil forfeiture of the defendant properties pursuant to 18 U.S.C. Section 981(a)(1)(C) (proceeds of wire fraud/wire fraud conspiracy) and 18 U.S.C. Section 981(a)(1)(A) (money laundering). It appears to the Court that proper proceedings for the issuance of this Final Order of Forfeiture have been had in this case as follows:

I. *Defendant Properties.*

The defendant properties in this case are as follows:

- 4,340,000 Tether ("USDT") cryptocurrency, valued at approximately $4,340,000.00, formerly associated with the cryptocurrency address beginning/ending 0xa17 . . . 44f0021 on the Ethereum blockchain. On or about June 21, 2024, the USDT tokens at the cryptocurrency address were frozen by Tether Limited Inc. ("Tether Limited"). Thereafter, pursuant to a federal seizure warrant issued by U.S. Magistrate Judge Jonathan D. Greenberg on August 21, 2024, Tether Limited "burned" the USDT tokens associated with the cryptocurrency address and, on or about November 20, 2024, reissued the equivalent amount of USDT tokens [namely, 4,340,000 USDT] to a U.S. law enforcement-controlled virtual currency wallet.

- 3,290,000 Tether ("USDT") cryptocurrency, valued at approximately $3,290,000.00, formerly associated with the cryptocurrency address beginning/ending 0x4e5 . . . d47abb5 on the Ethereum blockchain. On or about June 25, 2024, the USDT tokens at the cryptocurrency address were frozen by Tether Limited Inc. ("Tether Limited"). Thereafter, pursuant to a federal seizure warrant issued by U.S. Magistrate Judge Jonathan D. Greenberg on August 21, 2024, Tether Limited "burned" the USDT tokens associated with the cryptocurrency address and, on or about November 20, 2024, reissued the equivalent amount of USDT tokens [namely, 3,290,000 USDT] to a U.S. law enforcement-controlled virtual currency wallet.

- 577,578 Tether ("USDT") cryptocurrency, valued at approximately $577,578.00, formerly associated with the cryptocurrency address beginning/ending 0xafd . . . b2378a5 on the Ethereum blockchain. On or about June 21, 2024, the USDT tokens at the cryptocurrency address were frozen by Tether Limited Inc. ("Tether Limited"). Thereafter, pursuant to a federal seizure warrant issued by U.S. Magistrate Judge Jonathan D. Greenberg on August 21, 2024, Tether Limited "burned" the USDT tokens associated with the cryptocurrency address and, on or about November 20, 2024, reissued the equivalent amount of USDT tokens [namely, 577,578 USDT] to a U.S. law enforcement-controlled virtual currency wallet.

II. *Background.*

On February 27, 2025, the Complaint in Forfeiture (R. 1) was filed in this case against the defendant properties. Therein, the basic underlying facts of the case were alleged as follows:

a.) 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. (R. 1: Complaint in Forfeiture, at para. 30).

N.D. Ohio Victim.

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

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

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

e.) SUBJECT-1 then instructed A.H. as to what "platform" to use for the investments and where to transfer her purchased cryptocurrency. A.H. transferred the Crypto.com cryptocurrency to the address provided by SUBJECT-1 … . (*Id*., at para. 41).

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

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

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

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

j.) In total, between the initial $250,000.00 investment and the payment of "fees," A.H. lost approximately $663,352.00 in the scheme, constituting her entire life savings. (*Id*., at para. 46).

Michigan, California, Utah, and North Carolina Victims.

k.) **"B.D.", a resident of Michigan**, responded to a wrong number text on his phone. B.D. then exchanged texts back and forth with his new "friend" ("SUBJECT-2"), who told him that she was a female living in Seattle, Washington. SUBJECT-2 made promises of meeting B.D. in person, even sending him pictures of a plane ticket for a planned meeting in Chicago, Illinois. SUBJECT-2 cancelled the meeting before it occurred. After spending time exchanging texts and building a relationship, SUBJECT-2 suggested that B.D. invest in cryptocurrencies. (R. 1: Complaint in Forfeiture, at para. 47).

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

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

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

o.) B.D. lost approximately $11,996.00 from the investment scheme in which he was directed by SUBJECT-2. (*Id*., at para. 51).

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

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

r.) In or about May 2024, R.M. transferred the purchased cryptocurrency to the address recommended by SUBJECT-3, which R.M. believed to be the investment platform. After

R.M. was unable to retrieve his funds from the site, he further researched the "investment platform" and learned the website was created the day before he sent over his investment. (*Id*., at para. 54).

s.) R.M. lost approximately [$697,080.00] from the investment scheme in which he was directed by SUBJECT-3. (*Id*., at para. 55).

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

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

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

w.) M.S. lost approximately [$142,704.00] from the investment scheme in which he was directed by SUBJECT-4. (*Id*., at para. 59).

x.) **"H.L.", a resident of North Carolina**, responded to a wrong number text on her phone in December, 2023. H.L. then exchanged texts back and forth with her new "friend" ("SUBJECT-5"). After spending time exchanging texts and building a relationship, SUBJECT-5 suggested that H.L. invest in cryptocurrencies. (*Id*., at para. 60).

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

z.) When H.L. attempted to withdraw the funds from the "investment platform," she was told she had to pay different fees to access her funds. (*Id*., at para. 62).

aa.) H.L. lost approximately [$355,173.00] from the investment scheme in which she was directed by SUBJECT-5.

bb.) In total, A.H., B.D., R.M., M.S., and H.L. lost approximately [$1,870,305.00] in the investment fraud scheme. (*Id*., at para. 65).

Other Victims.

cc.) The above-described victims do not represent the entirety of identified victims. To date, [33] additional victims have been particularly identified. . . . In total [including A.H., B.D., R.M., M.S., and H.L.], the FBI has identified 38 victims/victim accounts. (R. 1: Complaint in Forfeiture, at para. 66).

dd.) In total, the 33 additional victims lost approximately $7,810,706.00 in the investment fraud scheme.

ee.) The identified loss to the 38 victims in the instant case is approximately $9,681,011.00.

Tracing Analysis.

ff.) Through several steps of "blockchain analysis," [1] the FBI was able to trace approximately $369,683.00 of A.H.'s total loss ($663,352.00) to the subject cryptocurrency addresses as follows:

address ending 44f0021: 314,657 USDT [2] ($314,657.00).
address ending d47abb5: 11,954 USDT ($11,954.00).
address ending b2378a5: 43,071 USDT ($43,071.00).

(*Id*., at para. 74).

---

[1] 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. (R. 1: Complaint in Forfeiture, at para. 26).

[2] 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. (*Id*., at para. 19).

gg.) Through several steps of "blockchain analysis," the FBI was able to trace approximately $11,101.00 of B.D.'s total loss ($11,996.00) to the subject cryptocurrency addresses as follows:

address ending 44f0021: 5,110 USDT ($5,110.00).
address ending d47abb5: 4,967 USDT ($4,967.00).
address ending b2378a5: 1,024 USDT ($1,024.00).

.

(*Id.*, at para. 76).

hh.) Through several steps of "blockchain analysis," the FBI was able to trace approximately $234,026.89 of R.M.'s total loss ($697,080.00) to the subject cryptocurrency addresses as follows:

address ending 44f0021: 227,963 USDT ($227,963.00).
address ending b2378a5: 6,063 USDT ($6,063.00).

.

(*Id.*, at para. 77).

ii.) Through several steps of "blockchain analysis," the FBI was able to trace approximately $136,047.74 of M.S.'s total loss ($142,704.00) to the subject cryptocurrency addresses as follows:

address ending d47abb5: 136,047 USDT ($136,047.00).

(*Id.*, at para. 78).

jj.) Through several steps of "blockchain analysis," the FBI was able to trace approximately $168,744.00 of H.L.'s total loss ($355,173.00) to the subject cryptocurrency addresses as follows:

address ending 44f0021: 73,619 USDT ($73,619.00).
address ending b2378a5: 95,125 USDT ($95,125.00).

(*Id.*, at para. 79).

kk.) As set forth above, A.H., B.D., R.M., M.S., and H.L. do not represent the entirety of victims identified in the investigation. With respect to the 33 additional victims, the FBI's investigation determined:

The 33 additional victims had a total of approximately 2,068,945 USDT ($2,068,945.00) end up in the cryptocurrency address ending 44f0021.

The 33 additional victims had a total of approximately 1,612,213 USDT ($1,612,213.00) end up in the cryptocurrency address ending d47abb5.

The 33 additional victims had a total of approximately 649,972 USDT ($649,972.00) end up in the cryptocurrency address ending b2378a5.

(*Id*., at paras. 81-82).

ll.) In total, approximately 2,690,294 USDT ($2,690,294.00) of victim funds can be traced to the cryptocurrency address ending 44f0021. On or about June 21, 2024, the USDT tokens at the address were frozen by Tether Limited. (*Id*., at para. 83).

mm.) In total, approximately 1,765,181 USDT ($1,765,181.00) of victim funds can be traced to the cryptocurrency address ending d47abb5. On or about June 25, 2024, the USDT tokens at the address were frozen by Tether Limited. (*Id*., at para. 84).

nn.) In total, approximately 795,255 USDT ($795,255.00) of victim funds can be traced to the cryptocurrency address ending b2378a5. On or about June 21, 2024, the USDT tokens at the address were frozen by Tether Limited. (*Id*., at para. 85).

oo.) Pursuant to federal seizure warrants issued on August 21, 2024, a total of 8,207,578 USDT tokens ($8,207,578.00) - formerly associated with the subject cryptocurrency addresses - were transferred by Tether Limited to a U.S. law enforcement-controlled virtual currency wallet. (*Id*., at paras. 7(a), 7(b), and 7(c).)

pp.) On February 27, 2025, the Complaint in Forfeiture (R. 1) was filed in this case against the defendant properties.

qq.) The identity of the owner(s) of the subject cryptocurrency addresses is unknown. Accordingly, with respect to ownership, the only information available to law enforcement is the subject cryptocurrency addresses themselves. (*Id*., at para. 86).

III. ***The Forfeitability of the Defendant Properties***.

The Complaint in Forfeiture (R. 1) relates to violations of 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. Sections 1956 and 1957 (money laundering), and conspiracy to commit such offenses, in violation of 18 U.S.C. § 371 and 18 U.S.C. § 1956(h).

A. Wire Fraud - 18 U.S.C. § 1343.

Title 18 U.S.C. § 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.

Under 18 U.S.C. § 981(a)(1)(C), any property - real or personal - which constitutes, or is derived from, proceeds traceable to an offense(s) constituting "specified unlawful activity" (SUA) is subject to forfeiture to the United States. Wire fraud (18 U.S.C. § 1343) and wire fraud conspiracy (18 U.S.C. § 371) are SUAs as defined in 18 U.S.C. § 1956(c)(7), with reference to 18 U.S.C. § 1961(l).

Paragraph 87 of the Complaint in Forfeiture (R. 1) sets forth the following:

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

B. Money Laundering.

Title 18 U.S.C. § 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."

Title 18 U.S.C. § 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."

Under 18 U.S.C. § 981(a)(1)(A), any property - real or personal - "involved in" or traceable to an offense in violation of 18 U.S.C. § 1956(a)(1)(B)(i) (concealment money laundering), 18 U.S.C. § 1957 (transactional money laundering), and/or 18 U.S.C. Section 1956(h) (money laundering conspiracy) is subject to forfeiture.

Paragraph 14 of the Complaint in Forfeiture (R. 1) states as follows:

> . . . [U]nder a money laundering theory of forfeiture, the government is not limited to forfeiting only the criminal proceeds involved in the money laundering

transaction.[3] 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.[4]

Paragraph 15 of the Complaint in Forfeiture (R. 1) states as follows:

> *"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.[5]

---

[3] *See, United States v. McGauley*, 279 F.3d 62, 75-76 (1st Cir. 2002) (distinguishing forfeiture under Section 982(a)(1) from a proceeds forfeiture; the money laundering forfeiture is broader and is not limited to the proceeds being laundered); and, *United States v. Coffman*, 859 F. Supp. 2d 871, 875 (E.D. Ky. 2012) ("Money laundering forfeiture pursuant to Section 982(a)(1) applies to a larger class of property than proceeds forfeiture under Section 981(a)(1)(C) because it applies to more than just the laundered property or proceeds from the laundered property."), *aff'd*, 574 Fed. Appx. 541 (6th Cir. 2014).

[4] *See, United States v. Cessa*, 872 F.3d 267, 273-274 (5th Cir. 2017) ("Property involved in an offense includes the money or other property being laundered (the corpus), any commissions or fees paid to the launderer, and *any property used to facilitate the laundering offense*") (emphasis in original); *United States v. Coffman*, 2014 WL 354632, at *3 (E.D. Ky. 2014) (following *McGauley*; third party cannot complain that the forfeited funds include money not derived from the defendant's fraud; the government's theory is that the defendant used the money to facilitate the money laundering offense); and, *United States v. Real Property Located at 6415 N. Harrison Ave.*, 2011 WL 2580335, at *4 n.1 (E.D. Cal. 2011) (denying motion to dismiss a forfeiture complaint; even if the property is only traceable in part to the proceeds of the underlying fraud, it is forfeitable in its entirety as property involved in the laundering of the fraud proceeds).

[5] *See, United States v. Huber*, 404 F.3d 1047, 1058 (8th Cir. 2005) (the SUA proceeds involved in a financial transaction, as well as any clean money commingled with it, constitute the corpus of the money laundering transaction; both are subject to forfeiture); *United States v. Coffman*, 859 F. Supp. 2d 871, 877 (E.D. Ky. 2012) (following *Huber*; explaining that untainted funds may be forfeitable either as the subject of a money laundering transaction or as facilitating property; when commingled funds are transferred in their entirety to another bank account, all of the funds are forfeitable as the subject of the transaction); and, *United States v. Funds on Deposit at Bank One, Indiana*, 2010 WL 909091, at *8 (N.D. Ind. 2010) (following *Huber*; when defendant commingled drug proceeds with other funds in a bank account, and transferred the commingled funds to another account, and commingled them yet again before making a third transfer, all of the funds involved in the last transfer were forfeitable as property involved in violations of 18 U.S.C. Sections 1956 and 1957).

Paragraph 16 of the Complaint in Forfeiture states as follows:

> *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.[6]

Paragraph 88 of the Complaint in Forfeiture (R. 1) sets forth the following conclusion:

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

---

[6] *See, United States v. Bikundi*, 926 F.3d 761 (D.C. Cir. 2019) (collecting cases and following other circuits in holding that untainted funds in a bank account are forfeitable as property involved in a money laundering offense if through commingling or shuffling tainted and untainted funds, defendant conceals the source of criminal proceeds); *United States v. Coffman*, 574 Fed. Appx. 541 (6th Cir. 2014) (following *McGauley*; commingled funds are forfeitable under a facilitation theory if the government shows that the defendant commingled the funds to facilitate his offense); *United States v. All Assets Held at Bank Julius Baer & Co. Ltd*., 2024 WL 3612982, at *23 n.19 (D.D.C. 2024) (complaint adequately alleged that all assets in commingled bank account were forfeitable under a money laundering theory because "otherwise untainted funds commingled with and used to conceal the source of tainted funds are generally forfeitable"); *United States v. Sterlingov*, 2023 WL 2387759 (D.D.C. 2023) (clean funds commingled with other funds in a bitcoin tumbling business facilitate the money laundering offense and so are forfeitable as property involved in money laundering, whether the clean money was the defendant's own money or other customers' money; collecting cases); and, *United States v. $70,150.00 in U.S. Currency*, 2009 WL 3614871, at *11 (S.D. Ohio 2009) (following *McGauley*; when government moves for summary judgment on a money laundering theory, it is irrelevant if some of the money in the bank account came from a legitimate source, because any such untainted funds would be forfeitable as property used to conceal or disguise the tainted funds in the account).

Paragraphs 89 and 90 of the Complaint in Forfeiture set forth the following conclusions:

> The transfers to [the subject cryptocurrency addresses] also constituted transactions in violation of 18 U.S.C. Section 1956(a)(1)(B)(i) (concealment money laundering). The blockchain analysis in this case demonstrated that the fraudsters moved the proceeds of the criminal activity through multiple financial accounts, sometimes at a rapid pace, with no discernable legitimate purpose. Such convoluted transactions that serve no apparent legitimate purpose imply that the purpose of the convoluted transactions was to conceal the nature, source, location, ownership, and control of the SUA proceeds.
>
> Under 18 U.S.C. Section 981(a)(1)(A), all property - real and personal - "involved in" or traceable to an offense in violation of § 1956(a)(1)(B)(i) is subject to forfeiture. Particularly, "other funds" in a cryptocurrency address into which SUA proceeds are transferred as part of a concealment money laundering offense - along with any "other funds" transferred with the SUA proceeds as part of the concealment money laundering offense - are subject to forfeiture as property "involved in" the offense. In both instances, the "other funds" commingled with the SUA proceeds obfuscate the origin or existence of the SUA proceeds. Therefore, all funds in [the subject cryptocurrency addresses] were "involved in" concealment money laundering.

IV. *The United States has satisfied all of the statutory notice requirements as set forth in Rule G(4) of the Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions.*

a.) The Complaint in Forfeiture (R. 1) was filed on February 27, 2025. As set forth above, this is an action for the civil forfeiture of the defendant properties under 18 U.S.C. Section 981(a)(1)(C) (proceeds of wire fraud/wire fraud conspiracy) and 18 U.S.C. Section 981(a)(1)(A) (money laundering).

b.) The Clerk of this Court issued a Warrant of Arrest *in Rem* on February 27, 2025, which was executed on the defendant properties by the United States Marshals Service (USMS) on March 3, 2025. (R. 6-1: Marshal's Return - Warrant of Arrest *in Rem*).

c.) Pursuant to Rule G(4)(a)(iv)(C) of the Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions ("Supplemental Rules"), the United States posted notice of the Complaint in Forfeiture on an official government internet site for at least 30

consecutive days, beginning on March 6, 2025 and ending on April 4, 2025. No claims to the defendant properties were filed as a result of the internet notification. (Docket Report).

d.) Under Supplemental Rule G(4)(b)(i), the owner of the cryptocurrency address ending 44f0021 was a potential claimant in the instant case. Supplemental Rule G(4)(b)(iii)(A) requires that notice of the action and a copy of the Complaint in Forfeiture "be sent by means reasonably calculated to reach the potential claimant." The identity of the owner of the cryptocurrency address ending 44f0021 is unknown. In this regard, the FBI's underlying investigation indicates that the criminal syndicates that operate the particular type of investment fraud scheme detailed in the Complaint in Forfeiture often operate from compounds in Cambodia and Myanmar. (R. 1: Complaint in Forfeiture, at para. 37). Therefore, the only information available to law enforcement as to the identity of the owner of the cryptocurrency address ending 44f0021 is the cryptocurrency address itself. (*Id*., at para. 86).

e.) On March 3, 2025 - pursuant to Supplemental Rule G(4)(b)(iii)(B) - FBI Special Agent Milan R. Kosanovich sent the wordage of the Notice of Forfeiture (R. 1-5) [7] - with a link

---

[7] The Notice of Forfeiture (R. 1-5) advised the owner of the cryptocurrency address ending 44f0021 as follows:

> The above-captioned forfeiture action was filed in U.S. District Court on February 27, 2025. A link to a copy of the Complaint in Forfeiture is provided. The following applies if you claim an interest in the defendant 4,340,000 Tether ("USDT") cryptocurrency, valued at approximately $4,340,000, formerly associated with cryptocurrency address . . . ending . . . 44f0021:
>
> Pursuant to Rule G of the Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions, you are required to file with the Court, and serve upon James L. Morford, plaintiff's attorney, whose address is United States Attorney's Office, 400 United States Court House, 801 West Superior Avenue, Cleveland, Ohio 44113, a verified claim to the defendant property within 35 days after your receipt of the complaint. The claim shall contain the information required by Rule G(5) of the said Supplemental Rules. Additionally, you must file and serve an answer to the complaint,

to a copy of the Complaint in Forfeiture - by message on the Ethereum blockchain to the cryptocurrency address ending 44f0021. The transmission of the message was successful in that SA Kosanovich received confirmation that the transaction was broadcast and confirmed to the Ethereum blockchain at 2:06 p.m. Eastern Time on March 3, 2025. (R. 3: Return of Service).

f.) Under Supplemental Rule G(4)(b)(i), the owner of the cryptocurrency address ending d47abb5 was a potential claimant in the instant case. The identity of the owner of the cryptocurrency address ending d47abb5 also is unknown. Therefore, the only information available to law enforcement as to the identity of the owner of the cryptocurrency address ending d47abb5 is the cryptocurrency address itself. (R. 1: Complaint in Forfeiture, at para. 86).

g.) On March 3, 2025 - pursuant to Supplemental Rule G(4)(b)(iii)(B) - FBI Special Agent Kosanovich sent the wordage of the Notice of Forfeiture (R. 1-6) [8] - with a link to a copy of the Complaint in Forfeiture - by message on the Ethereum blockchain to the cryptocurrency address ending d47abb5. The transmission of the message was successful in that SA Kosanovich received confirmation that the transaction was broadcast and confirmed to the Ethereum blockchain at 2:04 p.m. Eastern Time on March 3, 2025. (R. 4: Return of Service).

h.) Under Supplemental Rule G(4)(b)(i), the owner of the cryptocurrency address ending b2378a5 was a potential claimant in the instant case. The identity of the owner of the cryptocurrency address ending b2378a5 is unknown. Therefore, the only information available

---

> or a motion under Rule 12 of the Federal Rules of Civil Procedure, within 20 days after the filing of the claim, exclusive of the date of filing. If you fail to do so, judgment will be taken for the relief demanded in the complaint.

[8] The wordage of R. 1-6 (Notice of Forfeiture) and R. 1-5 (Notice of Forfeiture) is identical, with the exception of the different cryptocurrency addresses. The wordage of R. 1-5 is set forth above in footnote 7.

to law enforcement as to the identity of the owner of the cryptocurrency address ending b2378a5 is the cryptocurrency address itself. (R. 1: Complaint in Forfeiture, at para. 86).

i.) On March 3, 2025 - pursuant to Supplemental Rule G(4)(b)(iii)(B) - FBI Special Agent Kosanovich sent the wordage of the Notice of Forfeiture (R. 1-7) [9] - with a link to a copy of the Complaint in Forfeiture - by message on the Ethereum blockchain to the cryptocurrency address ending b2378a5. The transmission of the message was successful in that SA Kosanovich received confirmation that the transaction was broadcast and confirmed to the Ethereum blockchain at 2:13 p.m. Eastern Time on March 3, 2025. (R. 5: Return of Service).

j.) The owners of the cryptocurrency addresses ending 44f0021, d47abb5, and b2378a5 are the only known potential claimants to the defendant properties.

k.) The owners of the cryptocurrency addresses ending 44f0021, d47abb5, and b2378a5 have failed to file a verified claim to the defendant properties [as required by 18 U.S.C. § 983(a)(4)(A) and Supplemental Rule G(5)(a)] or an answer to the Complaint in Forfeiture [as required by 18 U.S.C. § 983(a)(4)(B) and Supplemental Rule G(5)(b)]. (Docket Report).

ACCORDINGLY, IT IS ORDERED, ADJUDGED, AND DECREED:

a.) The following properties are finally forfeited to the United States under 18 U.S.C. § 981(a)(1)(C) (proceeds of wire fraud/wire fraud conspiracy) and 18 U.S.C. § 981(a)(1)(A) (money laundering) and no right, title, or interest shall exist in any other party. The United States shall seize and take control of the properties and shall dispose of them in accordance with law:

---

[9] The wordage of R. 1-7 (Notice of Forfeiture) and R. 1-5 (Notice of Forfeiture) is identical, with the exception of the different cryptocurrency addresses. The wordage of R. 1-5 is set forth above in footnote 7.

- 4,340,000 Tether ("USDT") cryptocurrency (24-FBI-006720), valued at approximately $4,340,000.00, formerly associated with the cryptocurrency address beginning/ending 0xa17 . . . 44f0021 on the Ethereum blockchain.

- 3,290,000 Tether ("USDT") cryptocurrency (24-FBI-006725), valued at approximately $3,290,000.00, formerly associated with the cryptocurrency address beginning/ending 0x4e5 . . . d47abb5 on the Ethereum blockchain.

- 577,578 Tether ("USDT") cryptocurrency (24-FBI-006726), valued at approximately $577,578.00, formerly associated with the cryptocurrency address beginning/ending 0xafd . . . b2378a5 on the Ethereum blockchain.

b.) As set forth above, the identified loss to the 38 victims in the instant case is approximately $9,681,011.00. By this Final Order of Forfeiture, a total of approximately 8,207,578 Tether ("USDT") cryptocurrency, valued at approximately $8,207,578.00, is finally forfeited to the United States. Returning forfeited assets to victims through the remission process is one of the primary goals of the U.S. Department of Justice's Asset Forfeiture Program. *See*, DOJ Asset Forfeiture Policy Manual, at Chapter 14-1. Following the entry of this Final Order of Forfeiture, each victim will have the ability to submit a Petition for Remission or Mitigation to the U.S. Department of Justice, Criminal Division. Through the orderly remission process, all 38 identified victims will have the opportunity to recover their lost funds on a *pro rata* basis.

SO ORDERED this 8th day of May, 2025.

/S/ SOLOMON OLIVER, JR.
Solomon Oliver, Jr.
United States District Judge, N.D. Ohio