UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

United States of America,

Plaintiff,

Civil Case No. 25-cv-13121
Honorable
Magistrate Judge

vs.

266,907 Tether ("USDT") associated with cryptocurrency address 0x9798E11938DDf58f103410111c56dA9d2F00b9c8

Defendant *in Rem.*

Complaint for Forfeiture

Plaintiff, United States of America, by and through its undersigned attorneys, states the following in support of this Complaint for Forfeiture:

Jurisdiction and Venue

1. This is an *in rem* civil forfeiture action pursuant to 18 U.S.C. § 981(a)(1)(A) and 18 U.S.C. § 981(a)(1)(C), resulting from violations of 18 U.S.C. §§ 1343, 1956, and 1957.

2. This Court has original jurisdiction over this proceeding pursuant to 28 U.S.C. § 1345 because this action is being commenced by the United States of America as plaintiff.

3. This Court has jurisdiction over this forfeiture action under 28 U.S.C. § 1355(b)(1)(A) because acts giving rise to the forfeiture occurred in the Eastern District of Michigan.

4. Venue is proper before this Court under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the government's claims occurred in the Eastern District of Michigan.

5. Venue is also proper before this Court under 28 U.S.C. § 1395 because the action accrued in the Eastern District of Michigan.

Defendant *in rem*

6. The defendant *in rem* consists of the following "Defendant Cryptocurrency": 266,907 Tether ("USDT") associated with cryptocurrency address 0x9798E11938DDf58f103410111c56dA9d2F00b9c8 (25-USS-000189).

7. The Defendant Cryptocurrency was seized on May 6, 2025, as proceeds of wire fraud and/or money laundering pursuant to a seizure warrant executed by the United States Secret Service ("USSS").

Underlying Criminal Statutes

8. 18 U.S.C. § 1343 ("Wire Fraud") prohibits anyone from devising or intending to devise any scheme or artifice to defraud, or to obtain 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. 18 U.S.C. § 1956(a)(1)(B)(i) makes it a federal offense for anyone, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, to conduct or attempt to conduct 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, location, source, ownership, or control of the proceeds.

10. 18 U.S.C. § 1957 makes it unlawful for any person to knowingly engage or attempt to engage in a monetary transaction in criminally derived property of a value greater than $10,000 if the property is, in fact, derived from specified unlawful activity.

Statutory Basis for Civil Forfeiture

11. 18 U.S.C. § 981(a)(1)(A) provides for civil forfeiture of any property, real or personal, involved in a transaction or attempted transaction in violation of 18 U.S.C. §§ 1343, 1956, and 1957, or any property traceable to such property.

12. 18 U.S.C. § 981(a)(1)(C) provides for civil forfeiture of any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of a specified unlawful activity, which includes violations of 18 U.S.C.

§ 1343 (Wire Fraud), 18 U.S.C. § 1956 (Money Laundering), and 18 U.S.C. § 1957 (Spending).

Factual Basis in Support of Forfeiture

13. Virtual currency (also known as cryptocurrency or digital currency) is generally defined as an electronic-sourced unit of value that can be used as a substitute for fiat currency (i.e., currency created and regulated by a government). Virtual currencies exhibit properties similar to other currencies, but do not have a physical form, existing entirely on the internet. Virtual currency is not issued by any government or bank (in contrast with "fiat" or conventional currencies) and is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Virtual currency is legal in the United States and accepted for legitimate financial transactions. However, it is also used for conducting illegal transactions or for concealing or disguising the true nature, source, location, ownership or control of illegally obtained criminal proceeds.

14. A virtual-currency exchange (an "exchange") is a business that allows customers to trade virtual currencies for other virtual or fiat currencies. An exchange can be a brick-and-mortar business, or strictly an online business. Both brick-and-mortar and online exchanges accept a wide variety of virtual currencies, and exchange them for fiat and traditional payment methods, other virtual currencies, or transfers between virtual currency owners. Many exchanges are

located outside the boundaries of the United States to avoid regulation and legal requirements. One of the largest and most popular exchanges is Binance.

15. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, linked using cryptography, containing an immutable and historical record of every transaction. The blockchain is a decentralized, distributed, and public digital ledger that is used to record transactions across many computers in a way that the record cannot be altered retroactively without additionally changing all successive blocks and the consent of the network. Blockchain is a method to record transactions that provides high security by design: transactions are verified with advanced cryptography and spread across many computers in a peer-to-peer network or distributed ledger. The blockchain can be updated multiple times per hour and record 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.

16. Tokens are a form of digital asset that function similar to a virtual currency. Tokens are generally created by an issuing company and then used like currency by and within companies including the issuer, but are generally distinct from other blockchain-based cryptocurrencies such as Bitcoin. Digital tokens are often issued by companies attempting to launch a new digital product or digital

service, where investors purchase tokens for cash and expect that they will exchange these tokens at a later date for greater value if the issuer is successful. While tokens can be used as a limited form of payment, these tokens officially remain the property of the issuer, which often will maintain technical tools that can restrict such tokens from being transferred further. In this way, a token may be analogized to a voucher or I-O-U, in that they are not specifically a currency, but represent value and may be exchanged at that value. Many tokens can be bought and transferred within certain exchanges, such as Binance.

17. One popular and commonly used token is Tether ("USDT"), a token issued by Tether Limited. Tether is a decentralized, peer-to-peer form of virtual currency having no association with banks or governments. Users purchase USDT, which is stored in a user's digital or cryptocurrency wallet (a "wallet"). USDT is generally considered a "stablecoin," meaning that it is intended to closely approximate the value of the U.S. Dollar and thus can act as a virtual currency store of value similar to the U.S. Dollar. For this reason, cryptocurrency traders, both legitimate and illegitimate, will often convert other digital currencies into USDT for temporary or long-term storage, as by design, USDT typically does not experience the dramatic swings in value seen in other digital currencies.

18. A wallet is identified by unique electronic addresses that essentially stores the access code that allows an individual to conduct transactions on the

public ledger. To access a wallet on the public ledger, an individual must use a public address and a private address. The public address can be analogized to an account number while the private address is similar to a password used to access that account. Even though the public address of those engaging in virtual-currency transactions are recorded on the public ledger, the true identities of the individuals or entities behind the public address are not recorded. If a real individual or entity is linked to a public address, however, it may be possible to determine what transactions were conducted by that individual or entity. Therefore, digital transactions are often described as "pseudonymous," meaning they are partially anonymous. Most individuals are identified when they use a virtual-currency exchange to make a transaction between virtual currency and fiat currency, or through virtual-currency exchangers that voluntarily or through legal order, cooperate with law enforcement.

19. The cryptocurrency seized in this matter is largely derived from an investment-fraud scam commonly referred to as "pig butchering," perpetrated on victims throughout the United States, including in the Eastern District of Michigan. Pig-butchering schemes typically begin when a scammer sends a victim a seemingly innocuous or misidentified message. From there, the scammer will attempt to establish a more personal relationship with the victim by using manipulative tactics like those used in online romance scams.

20. The victims in pig-butchering schemes are referred to as "pigs" by the scammers because the scammers use elaborate storylines to "fatten up" victims into believing they are in a romantic or otherwise close personal relationship. Once the victim places enough trust in the scammer, the scammer typically entices the victim into a cryptocurrency investment scheme. The investment schemes are fake but have the appearance of a legitimate enterprise through the use of fabricated interfaces, derivative or "spoofed" websites that appear related to legitimate companies, and other techniques designed to bolster the scheme's legitimacy. This generally includes a fake investment platform operated through a website or mobile application that displays a fictitious investment portfolio with abnormally large investment returns.

21. The investment platforms are a ruse, and the funds contributed are always routed to a cryptocurrency address the scammers control (this is when the scammers refer to "butchering" or "slaughtering" the victims). When the victims do attempt to withdraw their funds, they are unable to do so and are often met with various excuses or even required to pay "taxes" in order to release their funds. Eventually, most victims are completely locked out of their accounts and lose all their funds.

22. The Defendant Cryptocurrency is forfeitable to the United States as property that constitutes or is derived from the proceeds of wire fraud in violation

of 18 U.S.C. § 1343 and as property involved in money laundering. The facts supporting this evidentiary determination include, but are not limited to, the following:

a. On or about September 19, 2023, the United States Secret Service Detroit Field Office ("USSS") learned that an individual, "V1", was the victim of an online cryptocurrency investment fraud.

b. V1 stated that she met an individual purporting to be "Jie Tang" on an online Chinese dating application, known as Jiayuan.com. Their conversation began with everyday cordial topics and involved video calls via the platform, Skype, then turned into conversation about investments and investing.

c. The victim, a resident of Leonard, Michigan, advised USSS that in the month of May 2023, Jie Tang suggested an investment opportunity in cryptocurrency, which involved making quick buys and sells of cryptocurrencies, guaranteeing trading success.

d. V1 was instructed to open an account with numerous cryptocurrency exchanges, such as Coinbase, Crypto.com, Gemini, Kraken, and Bitstamp. V1 was then directed to send the funds from Coinbase, Crypto.com, Gemini, Kraken, and Bitstamp to V1's Coinbase Wallet in order to send to "coinuppool.com".

e. Jie Tang helped V1 open the Coinbase Wallet and would provide step-by-step instructions for V1 to begin "trading" on the fictitious website, coinuppool.com.

f. Once Jie Tang convinced V1 to open an account with Coinbase, on May 8, 2023, V1 made an initial deposit of $3,000.00 via a wire transfer from Bank of America account #1068 (BOA 1068) to V1's cryptocurrency account with Coinbase.

g. V1 invested additional funds after the deposit of the initial $3,000.00 was successful. An analysis of BOA 1068 shows the following successful transactions between the BOA 1068 and V1's cryptocurrency accounts.

Date Sent	**Amount**	**Beneficiary**	**Notes**
05/08/2023	$3,000.00	Coinbase (Cross River Bank)	
05/11/2023	$9,900.00	Crypto.com (Metropolitan National Bank)	
05/12/2023	$9,950.00	Crypto.com (Metropolitan National Bank)	
05/25/2023	230,000.00	Southern Dress Inc. East West Bank Account #8072014924	Company Address: 99 Wall St, STE 4949 New York, NY 12207
06/01/2023	$7,000.00	Gemini (Chase Bank)	
06/06/2023	$72,000.00	Gemini (Chase Bank)	
06/08/2023	$165,000.00	Bitstamp (Customers Bank)	
06/09/2023	$240,000.00	Bitstamp (Customers Bank)	
TOTAL	**$736,850.00**		Approximate Amount
8/14/2023	$230,000.00	BOA 1068	BOA recalled the wire initially sent to Southern Dress Inc. on 05/25/2023.

h. V1 explained that they were unable to withdraw their funds and was instructed by Jie Tang to deposit an additional $462,883.96 USD to pay the taxes associated with the trading gains.

i. Once V1 realized they may have been victimized, they immediately contacted Bank of America (BOA) and requested the wire transfer of $230,000.00 USD on 05/25/2023 be reversed and on 8/14/2023, BOA successfully recalled the wire, and the $230,000.00 USD was returned to BOA 1068.

j. V1 sent a total of approximately $736,850.00 USD from BOA 1068.

k. After V1's Bitstamp account received the $165,000.00 USD deposit, the funds were then swapped from US dollars to Ethereum (ETH), which is a type of cryptocurrency; the amount of 88.38511092 ETH was then sent to V1's Coinbase Wallet on June 8, 2023.

l. V1 advised that the funds in Bitstamp were used to purchase ETH, then sent to V1's Coinbase Wallet, and then to other cryptocurrency addresses that were not in the name of, or under the control, of V1.

m. A review of records shows that the initial cryptocurrency withdrawals were sent to the same two deposit locations (cryptocurrency addresses) in all four cryptocurrency transactions in which three of the

transactions were then converted into other forms of cryptocurrencies through cryptocurrency services.

n. Once the funds left V1's Coinbase Wallet, they were no longer under the control of V1 but were under the control of unidentified subjects (at this time), who then used the funds for additional cryptocurrency purposes.

o. Using blockchain analysis, the USSS Investigative Analyst conducted an analysis of V1's Coinbase Wallet and traced the funds that were sent from V1's Coinbase Wallet, 0x6caE9695DF87dd358bCA5df26f0a66eA5d4D2b7d to ETH address, 0x4fC18F0902Db1500e1a37bf069Ce0F2a30Bcf3E0 (ETH f3E0).

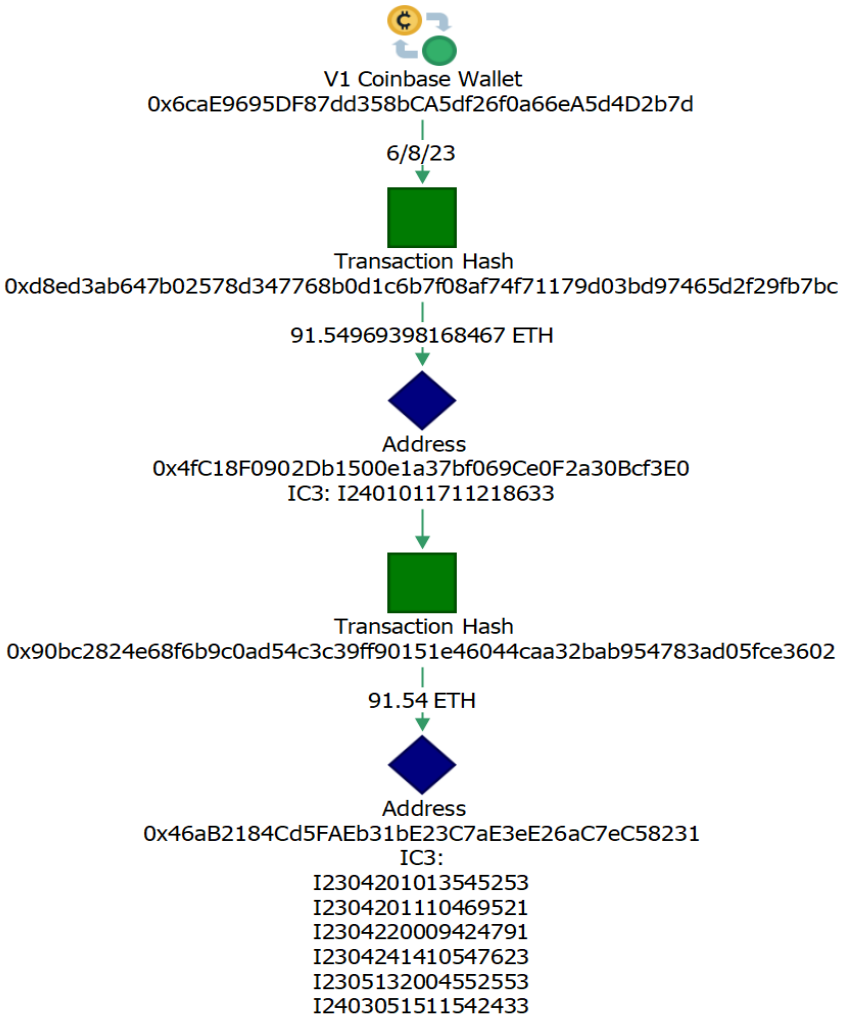
p. A review of records, in addition to the Cryptocurrency tracing conducted, showed the following transactions:

- $165,000.00 USD was sent from BOA 1068 to V1's Bitstamp account on June 8, 2023.
- Bitstamp received the funds in which they were converted to ETH and 88.38511092 ETH was sent to V1's Coinbase Wallet on June 8, 2023.
- V1's Coinbase Wallet received 88.379 ETH and sent approximately 91.55 ETH to Ethereum address, ETH f3E0. The

additional ETH is due to a previous balance prior to the 88.379 ETH deposit.

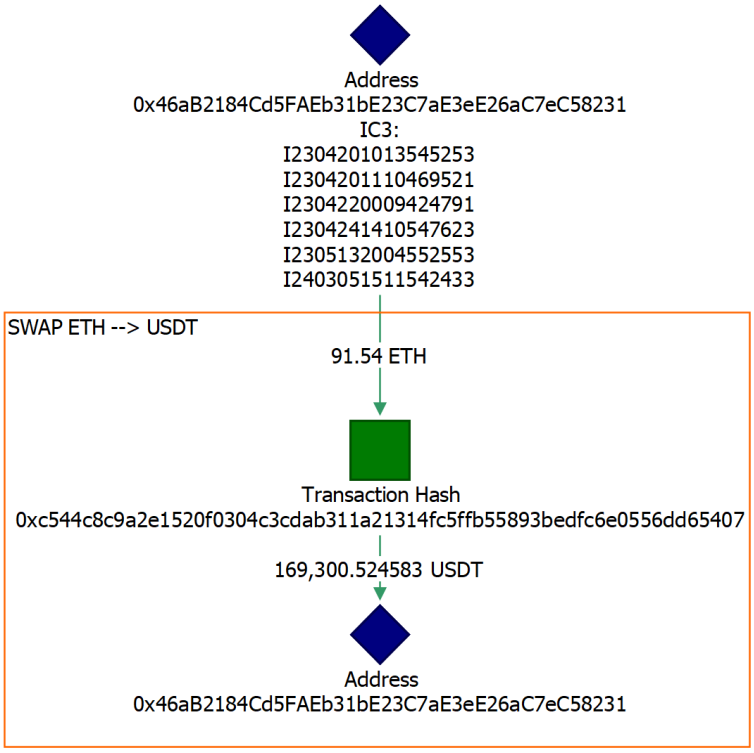
- ETH f3E0 received 91.54969398168467 ETH and sent 91.54 ETH to Ethereum address, 0x46aB2184Cd5FAEb31bE23C7aE3eE26aC7eC58231 (ETH 8231) on June 8, 2023. *See* Figure A.

Figure A:



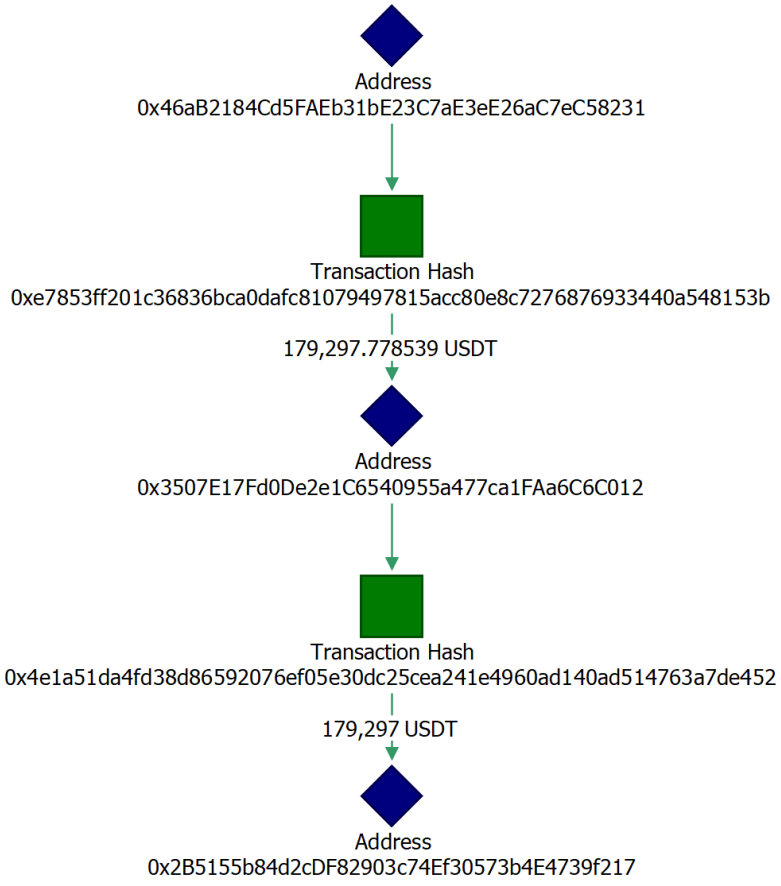
q. Blockchain analysis was conducted on ETH 8231 and revealed that the deposit of 91.54 ETH was swapped to a different cryptocurrency, specifically from ETH to USDT. ETH 8231 also received 5.352229677556038 ETH and 11,853.32065 USDT from V1's funds. Similarly to the 91.54 ETH, the 5.352229677556038 ETH was also swapped to USDT. More specifically, blockchain analysis shows that on June 8, 2023, a cryptocurrency "swap" took place in a transaction of swapping ETH for USDT through a swapping service called Tokenlon. ETH 8231 then held 169,300.524583 USDT. *See* Figure B.

Figure B:



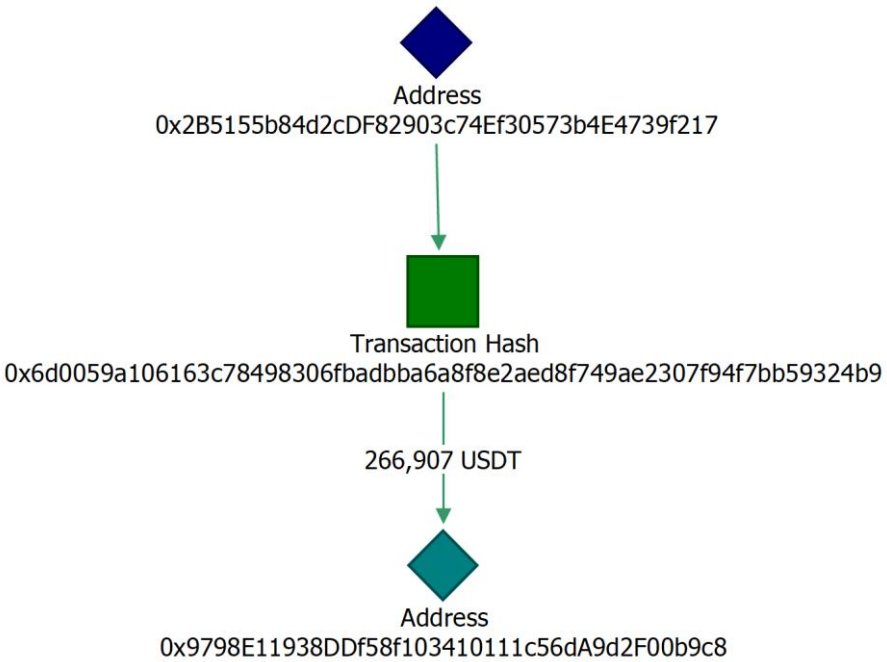
r. On June 8, 2023, after confirming the deposit of 169,300.524583 USDT into ETH 8231 through blockchain analysis, ETH 8231 sent 179,297.778539 USDT to Address, 0x3507E17Fd0De2e1C6540955a477ca1FAa6C6C012 (USDT C012). USDT C012 received funds on June 9, 2023, then sent 179,297 USDT to address, 0x2B5155b84d2cDF82903c74Ef30573b4E4739f217 (USDT f217). *See* Figure C.

Figure C:



s. On June 9, 2023, after confirming the deposit of 179,297 USDT into USDT f217, USDT f217 sent 266,907 USDT to Address, 0x9798E11938DDf58f103410111c56dA9d2F00b9c8 (USDT b9c8). The 266,907 USDT has remained unspent in USDT b9c8 since the deposit, which took place on June 13, 2023. USDT b9c8 is an un-hosted address through the Ethereum network, meaning the address is not connected to an exchange for cryptocurrency services. Upon voluntary assistance with Tether Holdings, the amount of 266,907 USDT was frozen by Tether Holdings on November 13, 2024. *See* Figure D.

Figure D:



t. Using the multiple addresses and swaps of virtual currency is indicative of "layering," which makes it difficult for law enforcement to properly identify the subjects involved, since the transactions are instantaneous and virtual.

u. USSS has determined that USDT b9c8 is being used as a recipient account for a portion of the funds fraudulently obtained from V1.

v. Research was conducted through the Internet Crime Complaint Center (IC3), which is a division of the Federal Bureau of Investigation that gives victims a convenient and easy way to report/alert authorities of criminal or civil violations on the internet.

w. Upon research through IC3, a victim from Fairfax, Virginia, filed a report indicating they were scammed into sending funds to ETH f3E0.

x. Additional research was conducted through IC3, and ETH 8231 has been identified as another cryptocurrency address reported in six (6) IC3 reports.

y. In all six (6) reports, victims are reporting that they sent funds to ETH 8231 in belief of an "investment" and were unable to withdrawal the funds, similarly to V1's scheme.

z. Most of these reports indicate the fictitious website coinuppool.com/coinatpool.com.

Claim

23. Plaintiff re-alleges and incorporates by reference each and every allegation contained in paragraphs one through 22 above, including all their subparts.

24. Based upon the facts outlined above and the applicable law, the Defendant Cryptocurrency is forfeitable to the United States under 18 U.S.C. § 981(a)(1)(A) and 18 U.S.C. § 981(a)(1)(C), as proceeds of wire fraud and as property involved in money laundering.

Conclusion and Relief

Plaintiff respectfully requests that a warrant for arrest of the defendant *in rem* be issued; that due notice be given to all interested parties to appear and show cause why the forfeiture should not be decreed; that judgment be entered declaring that the defendant *in rem* be condemned and forfeited to the United States of America for disposition according to law; and that the United States be granted such other relief as this Court may deem just and proper, together with the costs and disbursements of this action.

//

//

//

Respectfully submitted,

JEROME F. GORGON JR.
United States Attorney

S/Jasmine A. Moore
Jasmine A. Moore (P82181)
Assistant United States Attorney
211 W. Fort Street, Suite 2001
Detroit, MI 48226
(313) 226-9759
Jasmine.Moore@usdoj.gov

Dated: October 3, 2025

VERIFICATION

I, Timitre Kyriakides, am a Special Agent with the United States Secret Service. I have read the foregoing Complaint for Forfeiture and assert under penalty of perjury that the facts contained therein are true to the best of my knowledge and belief, based upon knowledge possessed by me and/or on information that I received from other law enforcement agents and/or officers.

Timitre Kyriakides, Special Agent
United States Secret Service

Dated: 10/2, 2025