UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

United States of America,

Civil Case No. 25-cv-13907
Honorable

Plaintiff,

vs.

2,700,000 Tether ("USDT") on the
Ethereum Network associated with cryptocurrency address
"0xA0D50E9b7EaaC04Ca82197a350fE3Ff1c24Bd13F"

Defendant *in Rem*.

Complaint for Forfeiture

Plaintiff, United States of America, by and through its undersigned attorneys, states upon information and belief 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": 2,700,000 Tether ("USDT") on the Ethereum Network associated with cryptocurrency address "0xA0D50E9b7EaaC04Ca82197a350fE3Ff1c24Bd13F" (25-IRS-001210).

7. The Defendant Cryptocurrency was seized pursuant to a seizure warrant executed on August 7, 2025, by Internal Revenue Service, Criminal Investigation (IRS-CI).

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 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 $10,000.00 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. §§ 1956 and/or 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).

Background on Virtual Currency and Cryptocurrency Confidence Scams

13. **Virtual Currency**: Virtual currencies are digital representations of value that, like traditional coin and paper currency, function as a medium of exchange (i.e., they can be digitally traded or transferred and can be used for payment or investment purposes). Virtual currencies are a type of digital asset separate and distinct from digital representations of traditional currencies, securities, and other traditional financial assets. The exchange value of a particular virtual currency generally is based on agreement or trust among its community of users. Some virtual currencies have equivalent values in real currency or can act as a substitute for real currency, while others are specific to particular virtual domains (e.g., online gaming communities) and generally cannot be exchanged for real

currency. Cryptocurrencies, like Bitcoin (or BTC), are types of virtual currencies, which rely on cryptography for security. Cryptocurrencies typically lack a central administrator to issue the currency and maintain payment ledgers. Instead, cryptocurrencies use algorithms, a distributed ledger known as a blockchain, and a network of peer-to-peer users to maintain an accurate system of payments and receipts.

14. **Blockchain**: A blockchain is a digital ledger run by a decentralized network of computers referred to as "nodes." Each node runs software that maintains an immutable and historical record of every transaction utilizing that blockchain's technology. Many digital assets, including virtual currencies, publicly record all their transactions on a blockchain, including all of the known balances for each virtual currency address on the blockchain. Blockchains consist of blocks of cryptographically signed transactions, and blocks are added to the previous block after validation and after undergoing a consensus decision to expose and resist tampering or manipulation of the data. There are many different blockchains used by many different virtual currencies. For example, Bitcoin in its native state exists of the Bitcoin blockchain, while Ether exists in its native state on the Ethereum network. Law enforcement can trace transactions on blockchains to determine which virtual currency addresses are sending and receiving particular virtual currency.

15. **Virtual Currency Address**: A virtual currency address is an alphanumeric string that designates the virtual location on a blockchain where virtual currency can be sent and received. A virtual currency address is associated with a virtual currency wallet.

16. **Private wallets**: non-custodial wallets, meaning the owner, as opposed to the host, controls the private keys and therefore all associated funding without oversight or financial regulation.

17. **Intermediary Address**: An "intermediary address" in virtual currency tracing refers to a wallet address used in a virtual currency transaction that acts as a temporary stopping point between the original sender and the final recipient, often employed to obscure the true source or destination of funds by adding an extra layer of complexity to the transaction trail. Essentially, criminal actors use intermediary addresses as "middleman" addresses to obfuscate the flow of funds. The funds are transferred through the middleman/intermediary address for no legitimate purpose. This is especially obvious because each transfer requires fees, meaning it costs the criminal actors money to do these transactions.

18. **Swaps**: Swaps of cryptocurrency are methods used to promote obfuscation on the blockchain and strengthen money laundering tactics to avoid law enforcement intervention. Tokenlon is an Asia based service that charges for controllers to token swap their coins. Tokelon is run and utilized by illicit actors to

promote money laundering; the service does not require any identification documents and is in countries that are free from the reach of most Financial Action Task Force.

19. **Tether ("USDT")**: is a cryptocurrency "stablecoin" issued by Tether Ltd. Tether Ltd. reports to back the issued USDT token with an equivalent number of United States dollars. The USDT token is approximately valued at an exchange rate of 1:1 with the United States dollar. USDT is a layer 2 token, that is hosted on other blockchains such as Ethereum and Tron blockchains, among others. Like other virtual currencies, if USDT is sent to and received from an address, the address will be a part of the specified blockchain the USDT smart contract was deployed on. If a transaction involves USDT deployed on ETH, an ETH address will be used to receive and send the USDT. If a transaction involves USDT on Tron, a Tron address will be used to send receive and send the USDT, USDT on ETH cannot directly transact with USDT on Tron as they are deployed on different blockchains. A USDT on ETH address is analogous to a bank account number and is represented as a 42-character string of letters and numbers. Users can operate multiple USDT on ETH addresses at any given time, with the possibility of using a unique USDT on ETH address for every transaction.

20. **Cryptocurrency confidence scams**: are commonly known as "Pig Butchering," are a type of internet-based cryptocurrency investment scam in which

the victim is "fattened up prior to slaughter." These scams are also referred to as cryptocurrency investment fraud. These types of scams typically involved four stages. First, a perpetrator cold contacts a victim via text, social media, or some other communication platform. Second, the perpetrator will establish a relationship with the victim by continuing to message them over days, weeks, or months. Third, the scammer will concoct a narrative to induce the victim to send them a series of purported investments, often in the form of cryptocurrency. These payments are often made through fraudulent investment platforms introduced by the scammer, which the victim believes to be legitimate. Fourth, after the victim stops sending additional payments, or begins to question the scammer about legitimacy of their "investments," the perpetrator cuts off all contact.

Factual Basis in Support of Forfeiture

21. 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, in violation of 18 U.S.C. §§ 1956, 1957. The facts supporting this evidentiary determination include, but are not limited to, the following:

a. On or about June 10, 2024, IRS-CI was notified by Shelby Township Police that a resident of Shelby Township, Michigan (V1) was the victim of an online cryptocurrency investment fraud scheme.

b. In early 2024, V1 was contacted by an individual calling themselves Kamia Holmes (Holmes) on WhatsApp. Holmes claimed to be a representative of the "BHG Investment platform". Holmes convinced V1 to begin investing money in "coin mining" on the BHG platform.

c. Holmes instructed V1 to open an account with the cryptocurrency platform Payward Ventures (Kraken) and to then transfer cryptocurrency to the BHG phone application.

d. Between February 9, 2024 and May 17, 2024, in a series of 20 transactions, V1 sent $668,100.00 United States Dollars (USD) to Kraken from their personal Bank of America (BOA) account.

e. V1 then converted the funds on Kraken to Ethereum ("ETH") and USDT and sent the cryptocurrency to their new private wallets on BHG, which V1 believed to be a legitimate cryptocurrency trading platform.

f. As shown in the table below, in a series of 26 withdrawals, V1 withdrew approximately 182.73 ETH and 80,262 USDT from their Kraken account to their private BHG wallets:

Date Sent	Transaction Hash	Amount	Cryptocurrency
2/13/2024 1:47	0x868771f750fd63fe56b4137a35014214f0b13f571f8fdaada4b9c43da75345a9	0.360798	ETH
2/14/2024 0:18	0x49de58edf8b86618336c96e29d8e04b40636872ab712f5327ad0546f01dd5b2e	49.9685	USDT
2/14/2024 1:58	0xfd548bdff4a91cf274c1267764d25f9bf147e98fcf8e15c4bca396f75bdfd68b	3.704829	ETH
2/19/2024 4:41	0x7550b8617eed104237dbe09c0eaf7ab82f2a40addf26112942c61cf99cc984fc	33.1167	USDT

2/25/2024 0:43	0x8ef2522b86e7c7ba9c1578f04a1fd8f015835bb75924dbc78e0ad006e6d89bce	0.155427	ETH
3/1/2024 18:05	0xb6d0448b2d1333c6cae513d60751a68fb621d6665535fb493ce8cf648ec8aaae	11.66684	ETH
3/5/2024 0:05	0x28625401b483f899d2fbafecd2f758cb16636d1db190a58fe9634aa3df976234	4940.721	USDT
3/22/2024 1:22	0xf0cd80f19e4d1b8a40d38e8117688b52ce887b1e2832e9721ea951531b794d75	14.02032	ETH
3/29/2024 0:36	0xf38e68bd0a35e310fd6c250b2eddd785ff621ee2e5a74f8e7de1fe1ec7d138c5	6.7	ETH
3/30/2024 1:57	0x679c4d40dd16e1737e1b5db5d58ff26898f72412020f8e65076edba1d2d0dfd7	1.531844	ETH
4/6/2024 19:35	0x31329b823f2a6a08a1800ccf0952790e1ac385d079ddc9ccb9ed48eb20846a3c	23.37066	ETH
4/16/2024 23:14	0x7bcd8ca2b3d6cbb2c1072c6c376df9c2127a1dbdc7978bf133427aca573d0139	4897.992	USDT
4/16/2024 23:47	0xa25a2bfcbfaa4d68d7b35fd2a0ad717d4c332059cdf1f3d9c023a0e6e4960dc9	498.2637	USDT
4/17/2024 0:09	0x7e07488a5beb5a7593b792b163fb1ca98df7fa6b2fcc1014b453ad681cc36a45	42.8	USDT
4/17/2024 18:33	0xc610fd6a28b762f0dad29264b1e0c6e9d9a28a45c70100b7d3f2caf2ad899d5d	2999.97	USDT
4/17/2024 23:15	0xec168bc0856a13c231298eb4036074911354153cec8a40e76b13c3ea5d98de9b	789	USDT
4/17/2024 23:15	0xec168bc0856a13c231298eb4036074911354153cec8a40e76b13c3ea5d98de9b	789	USDT
4/17/2024 23:15	0xec168bc0856a13c231298eb4036074911354153cec8a40e76b13c3ea5d98de9b	789	USDT
4/18/2024 13:15	0xce1a3cfbc6899be6e28d2b32dc6fafcef38715145f9bb97196998ef2719933b9	636.3184	USDT
4/19/2024 0:27	0xc121a40635ec91aa3638496d5222791e2cf2b839f4c48b93d2995881fa682483	48.37992	ETH
4/23/2024 19:19	0xbfd40862b2c10c42abcbe129609586ac7fc597a5da2320b7c064bb64703f1d7b	9899.533	USDT
4/25/2024 0:39	0x276de5bafb8dd1a45e51f026b0340412c15289b1b3a01f06c8f7bfc6eaed39c5	18.72877	ETH
4/26/2024 13:53	0xca355135754bde99109dd8561752f1a7a227b228afb021f319ea2f8263096ff2	24771.98	USDT
5/2/2024 0:52	0x4cc8ce29ca94bf2b430df4b3ffff28d01b1bc522378f0f83befc1fdbba7dda97	13.37585	ETH
5/3/2024 14:53	0x4c724199e5543586ca64cbf4ace1a92ac2fdf78ff627c284acec84d4911ffd65	32.20534	ETH
5/13/2024 16:20	0x4013eed74f052395f6c9f8ae344b1cb7fb3cb523d499d506a5853d04cce2a5dc	10400.42	USDT
5/15/2024 0:31	0x2ef39493fa525fa55af3867687320b2adacf2f7c133d7498bfa944947a15b9b2	8.531072	ETH
5/17/2024 23:36	0xfb8dd96488b69b321cc2c56939b6c760d566816504125e5e3faa953b242cd63d	20301.94	USDT

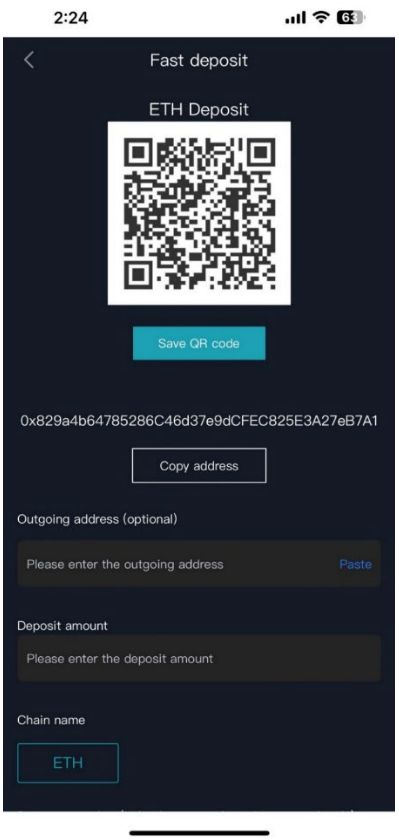
g. The fraudulent BHG application inaccurately showed V1 that they were profiting from their trades. Initially, V1 was also able to make three withdrawals from their private wallets on the BHG platform. V1 sent the withdrawn funds back to their personal Kraken account.

h. Holmes persuaded V1 to send their USDT to wallet "0x1ee100aEA22acb52fAFB24Bb2Cbbf3C738F70006". In a series of 10 withdrawals, V1 sent approximately 80,262 USDT from their private BHG wallet to wallet "0x1ee100aEA22acb52fAFB24Bb2Cbbf3C738F70006". This wallet was not in the name of, or under the control, of V1. Once the USDT was sent from V1's private wallet, the funds were no longer under their control.

i. All V1's USDT received by wallet "0x1ee100aEA22acb52fAFB24Bb2Cbbf3C738F70006" was withdrawn through a significant volume of low value transactions, apparently intended to obscure the destination of V1's USDT.

j. Holmes provided a deposit address for V1 to send the ETH to via the BHG phone application (*see* **Figure 1**).

Figure 1:



Fast deposit

ETH Deposit

0x829a4b64785286C46d37e9dCFEC825E3A27eB7A1

Outgoing address (optional)

Please enter the outgoing address

Deposit amount

Please enter the deposit amount

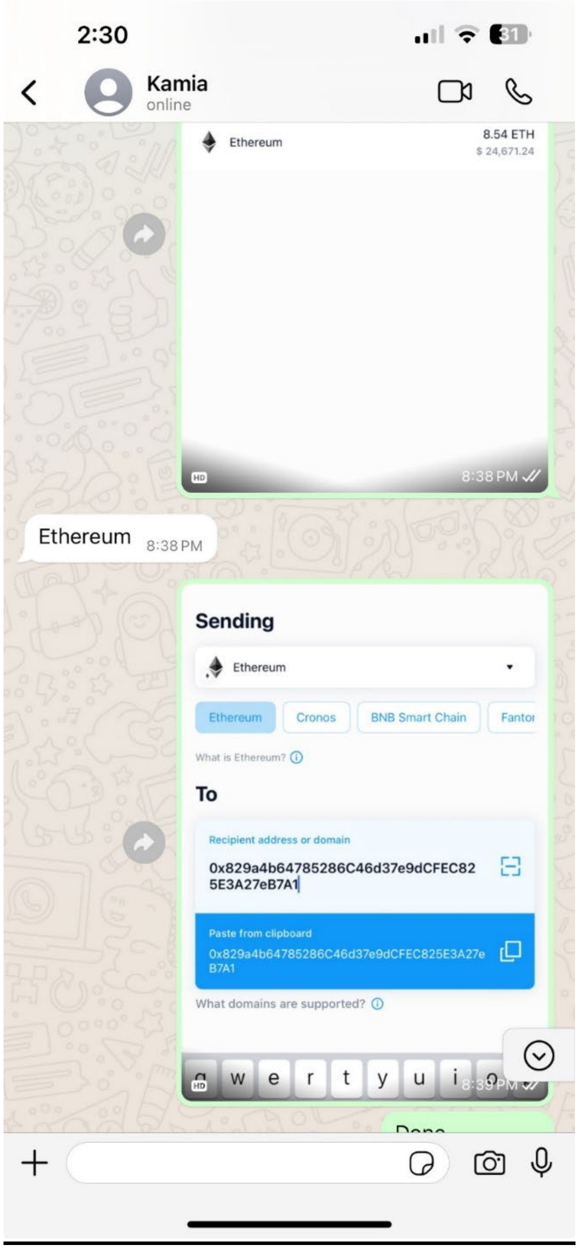
Chain name

ETH

k. From V1's private BHG wallet, in a series of 10 withdrawals, V1 sent approximately 181.34 ETH to the wallet "0x829a4b64785286C46d37e9dCFEC825E3A27eB7A1" ("Wallet B7A1"). This wallet was not in the name of, or under the control, of V1.

l. Holmes had V1 send screenshots of the transactions to enable Holmes to monitor the activity (*see* **Figure 2**).

Figure 2:



Ethereum 8.54 ETH
$ 24,671.24

8:38 PM

Ethereum 8:38 PM

Sending

Ethereum

To

Recipient address or domain

0x829a4b64785286C46d37e9dCFEC82
5E3A27eB7A1

Paste from clipboard

0x829a4b64785286C46d37e9dCFEC825E3A27e
B7A1

8:39 PM

Done

m. Once the ETH was sent from V1's private BHG wallet, the ETH was no longer under V1's control.

n. Using blockchain analysis and tracing software, IRS-CI traced V1's ETH utilizing the "last in first out" (LIFO) accounting principle, which assumes that the last, or more recent, incoming assets are the first expended or sent out. The tracing shows the following transactions connecting V1’s ETH to the Defendant Cryptocurrency (*see also* **<u>Figure 3</u>** below).

- On March 1, 2024, V1 wired $41,000.00 USD from their BOA account to their Kraken account.
- On March 1, 2024, V1 received the $41,000.00 to their Kraken account and converted the USD to approximately 11.66 ETH.
- On March 1, 2024, V1 withdrew approximately 11.66 ETH to their private BHG wallet “0x4C2504EB00aCd7EF36cB6bCdEBcb9F3E96227D41”.
- On March 1, 2024, at 07:54:35 PM UTC, V1 sent approximately 11.66 ETH to Wallet B7A1; the transaction ID on the ETH blockchain is “0x59b886832067348fc868feb0a3e2c61a664d5e1e58325e1fa4dbf8a2a4d479bd”. At this point, V1’s ETH was no longer under their control.
- On March 1, 2024, at 07:58:23 PM UTC, the decentralized exchange Tokenlon Smart Contract was used to swap the approximately 11.66 ETH to approximately 39,839 USDT.

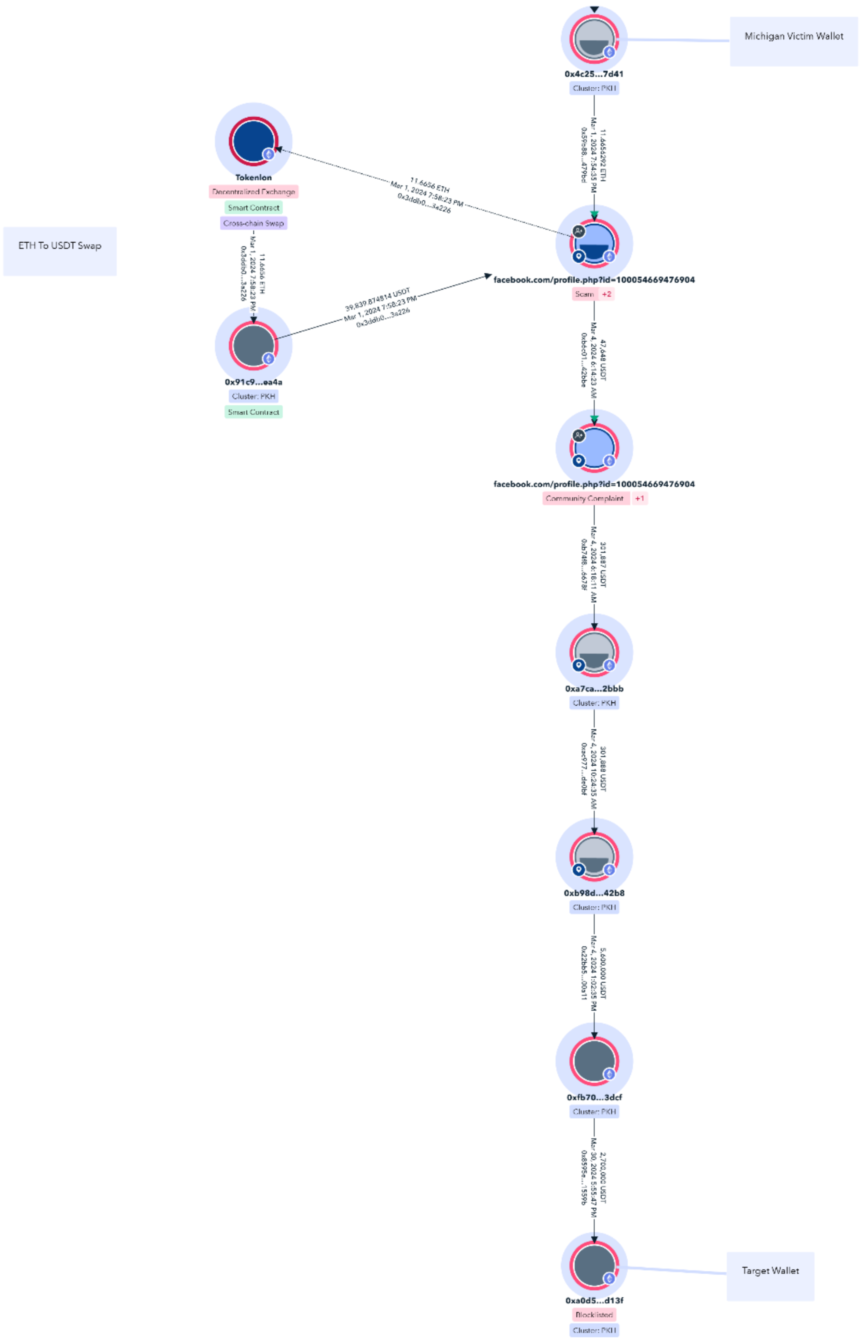
- On March 4, 2024, at 06:14:23 AM UTC, approximately 47,648 USDT was sent from Wallet B7A1 to wallet “0x17F8a4311E022AaaD40C7E79db2bC0d66d498481,” the transaction ID on the ETH blockchain is “0xb6c01de723ff6902ad63adb9ebd5d954768da8bc5dfed4374e8e83cb9d442bbe”.
- V1’s USDT was then consolidated with other funds in another wallet and then rapidly transferred into and out of more intermediary wallet addresses before being transferred to the Defendant Cryptocurrency:
- On March 4, 2024, at 06:18:11 AM UTC, wallet “0x17F8a4311E022AaaD40C7E79db2bC0d66d498481” sent approximately 301,887 USDT to wallet “0xa7CAeca20C5796E0274f13Db966c5032F4062bBb,” the transaction ID on the ETH blockchain is “0xb74f864ba42a3ece52e0171f6ab7a8c8d3c58db2ef85dd80d9c8302c2db6678f”.
- On March 4, 2024, at 10:24:35 AM UTC, wallet “0xa7CAeca20C5796E0274f13Db966c5032F4062bBb” sent approximately 301,888 USDT to wallet

“0xB98D357E5fd67320CD714DdeB918016D1c4242b8,” the transaction ID on the ETH blockchain is ”0xac977c4815c081d0d13b5ae027c3b067450a180f825b9fcee358ae2a84bde0bf”.

- Again, V1’s USDT was consolidated with other funds in wallet “0xB98D357E5fd67320CD714DdeB918016D1c4242b8,” and then rapidly transferred into and out of more intermediary wallet addresses before being transferred to the Defendant Cryptocurrency.
- On March 4, 2024, 01:02:35 PM UTC, wallet “0xB98D357E5fd67320CD714DdeB918016D1c4242b8” sent approximately 5,600,000 USDT to wallet “0xfB70212A81829AbEb53f75Ce2A62b91577153dcf,” the transaction ID on the ETH blockchain is ”0x22bb51bc9a38970af3de5787136cd073c801f7ce288e37df565db52d8bf00a11”.
- On March 30, 2024, 05:55:47 PM UTC, wallet “0xfB70212A81829AbEb53f75Ce2A62b91577153dcf” sent approximately 2,700,000 USDT to wallet “0xA0D50E9b7EaaC04Ca82197a350fE3Ff1c24Bd13F,” (the

wallet address containing the Defendant Cryptocurrency) the transaction ID on the ETH blockchain is ”0x8595eaedc73de2fdf5daaa19f2506511e0715d5b3b18aeccb83d82b4c131559b”.

Figure 3


Michigan Victim Wallet
0x4c25...7d41
Cluster: PKH
11.6656292 ETH
Mar 1, 2024 7:54:35 PM
0x59b88...479bd
Tokenlon
Decentralized Exchange
Smart Contract
Cross-chain Swap
11.6656 ETH
Mar 1, 2024 7:58:23 PM
0x3ddb0...3a226
ETH To USDT Swap
11.6656 ETH
Mar 1, 2024 7:58:23 PM
0x3ddb0...3a226
0x91c9...ea4a
Cluster: PKH
Smart Contract
39,839.874814 USDT
Mar 1, 2024 7:58:23 PM
0x3ddb0...3a226
facebook.com/profile.php?id=100054669476904
Scam
+2
47,648 USDT
Mar 4, 2024 6:14:23 AM
0xb6c01...42bbe
facebook.com/profile.php?id=100054669476904
Community Complaint
+1
301,887 USDT
Mar 4, 2024 6:16:11 AM
0xb74f8...6678f
0xa7ca...2bbb
Cluster: PKH
301,888 USDT
Mar 4, 2024 10:24:35 AM
0xac977...de0bf
0xb98d...42b8
Cluster: PKH
5,600,000 USDT
Mar 4, 2024 1:02:35 PM
0x22bb5...00a11
0xfb70...3dcf
Cluster: PKH
2,700,000 USDT
Mar 30, 2024 5:55:47 PM
0x8595e...1559b
Target Wallet
0xa0d5...d13f
Blocklisted
Cluster: PKH

o. Private addresses were utilized for the token movements described above, which is indicative of money laundering tactics that are used to conceal and disguise the original source of the funds.

p. As described above, V1's ETH was swapped to USDT on the Tokenlon decentralized exchange approximately four minutes after it was received. After the swap, the funds moved between wallets four times, each transaction consolidated with additional funds. Using cryptocurrency swaps and conducting numerous transactions within a short period of time are methods to conceal or disguise the source of the funds. The number of hops described in the preceding paragraphs are a strong indication that V1's funds were moved in a manner intended to conceal or disguise their nature, location, source, ownership, or control.

q. Additionally, the wallet address containing the Defendant Cryptocurrency was significantly funded with deposits of USDT consistent with the pattern described above (including multiple hops and short intervals of time between transactions).

r. 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. Wallet B7A1 and BHG have been identified in three IC3 reports, in addition to the reports filed by V1. Two IC3 reports reference the fraudulent investment platform BHG, one additional report identified Wallet B7A1 with a different alleged fictitious investment platform "MAXEXLLC.COM". In all three of these reports the victims reported being lured into sending funds after being contacted by someone online, in two of the reports the victims sent funds and were unable to withdrawal funds, similar to what happened to V1 (*See* **Figure 4**).

Figure 4

IC3 Complaint #	**Report Date**	**City/State of Victim**	**Approximate Loss Amount**	**"Investment" Platform**
I24011814044452143	1/18/2024	Richmond TX	$150,000.00	BHGBase
I2401192146076493	1/19/2024	Dorchester SC	$0.00	BHGBase
I2403230413246273	3/23/2024	Hayward CA	$8,877.00	MAXEXLLC.CO M

s. Tether Holdings voluntarily froze the Defendant Cryptocurrency on April 5, 2025, via ETH transaction ID "0xc47ff783d3be865a5596fbd0410a46e896be19a6cb549c0e408edb4386a393cc".

t. On August 7, 2025, a seizure warrant was issued by a federal magistrate judge in the Eastern District of Michigan to seize Defendant Cryptocurrency and was executed by IRS-CI.

Claim

22. Plaintiff re-alleges and incorporates by reference each and every allegation contained in paragraphs one through 21 above, including all their subparts.

23. 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 defendants *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, J.R
United States Attorney

*s/Kelly Fasbinder*___________
Kelly E. Fasbinder (P80109)
Assistant United States Attorney
211 W. Fort St., Ste. 2001
Detroit, MI 48226
(313) 226-9520
Kelly.Fasbinder@usdoj.gov

Dated: December 5, 2025

VERIFICATION

I, Ian Shane McDonald, am a Special Agent with IRS Criminal Investigations. 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.

Ian Shane McDonald, Special Agent
IRS Criminal Investigations

Dated: December 5, 2025