UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

United States of America, Plaintiff v. All USDT associated with the cryptocurrency address TEYbEC12AY5VdQi8EzKZtnB4Mu2KQmC2Vu; All USDT associated with the cryptocurrency address TQtn78tDLgEChRZ3u2BuC2UGyG3DPCEfbm; All USDT associated with the cryptocurrency address TMN7YCvqhgZeHiAZSULwGPgsAyh45R1nAM; All USDT associated with the cryptocurrency address TDbZVZbGZuAVC6D1sRwSr6kAZ6HVP22pFa; All USDT associated with the cryptocurrency address THrsQcq5epM7qLvQ7vUjZZxoZoh6YPsj4n; and All USDT associated with the cryptocurrency address TB9232EjpG3SRjsfqjBRxuenqDE1p1yQAm; and All USDT associated with the cryptocurrency address TYR4wmJx7rqZuKUvTUJBUdR7weDtPbKW1t, Defendants *in Rem*.	)	Civil Action No. 26-cv-11061

VERIFIED COMPLAINT FOR FORFEITURE *IN REM*

The United States of America, by its attorney, Leah B. Foley, United States Attorney for the District of Massachusetts, in a civil action of forfeiture *in rem* pursuant to 18 U.S.C.

§ 981(a)(1)(A) and Supplemental Rule G of the Federal Rules of Civil Procedure for Admiralty or Maritime Claims and Asset Forfeiture Actions, alleges that:

NATURE OF ACTION

1. This action is brought by the United States of America pursuant to 18 U.S.C. § 981(a)(1)(A), seeking civil forfeiture of the following USDT (Tether)[1]:

a. Approximately $103,367.252244 USDT, associated with the cryptocurrency address TEYbEC12AY5VdQi8EzKZtnB4Mu2KQmC2Vu ("Target Wallet 1");

b. Approximately $64,158.560977 USDT, associated with the cryptocurrency address TQtn78tDLgEChRZ3u2BuC2UGyG3DPCEfbm ("Target Wallet 2");

c. Approximately $33,098.57425 USDT, associated with the cryptocurrency address associated with the cryptocurrency wallet with address TMN7YCvqhgZeHiAZSULwGPgsAyh45R1nAM ("Target Wallet 3");

d. Approximately $34,035.068946 USDT, associated with the cryptocurrency address associated with the cryptocurrency wallet with address TDbZVZbGZuAVC6D1sRwSr6kAZ6HVP22pFa ("Target Wallet 4");

e. Approximately $48,022.47727 USDT associated with the cryptocurrency address THrsQcq5epM7qLvQ7vUjZZxoZoh6YPsj4n ("Target Wallet 5");

f. Approximately $5,013.084574 USDT, associated with the cryptocurrency address TB9232EjpG3SRjsfqjBRxuenqDE1p1yQAm ("Target Wallet 6"); and

g. Approximately $40,149.047216 USDT, associated with the cryptocurrency address TYR4wmJx7rqZuKUvTUJBUdR7weDtPbKW1t ("Target Wallet 7")

(collectively, the "Defendant Properties").

2. On August 14, 2025, the government obtained seizure warrants in connection with a Federal Bureau of Investigation ("FBI") investigation into group of unknown subjects (the "Target Subjects") who engaged in a cryptocurrency investment fraud scheme and money laundering

[1] USDT is a stablecoin. Each USDT token is worth approximately $1.00 USD and claimed to be backed by $1.00 USD in physical reserves. Payments or transfers of value made with USDT are recorded in the blockchain network.

operation that targeted at least one Massachusetts victim. To seize the applicable USDT, Tether Limited will "burn" (*i.e.*, destroy) the USDT tokens currency associated with the cryptocurrency wallet and reissue the equivalent amount of USDT tokens and transfer that equivalent amount to a government-controlled cryptocurrency wallet. In accordance with this process, Tether transferred the Defendant Properties to a U.S. government-controlled wallet on or about October 7, 2025.

3. As set forth in the subsequent paragraphs, the Defendant Properties constitute proceeds of Money Laundering, in violation of 18 U.S.C. §§ 1956(a)(1)(B)(i) and 1956(h). Therefore, all funds that existed in wallets that contain the Defendant Properties on the date of seizure are subject to forfeiture.

JURISDICTION AND VENUE

4. This Court has jurisdiction in this matter pursuant to 28 U.S.C. §§ 1345 and 1355. Venue is proper pursuant to 28 U.S.C. §§ 1355(b)(1) and 1395 because acts and omissions giving rise to the forfeiture occurred in the District of Massachusetts.

STATUTORY AUTHORITY

5. Pursuant to 18 U.S.C. § 981(a)(1)(A), the following property is subject to civil forfeiture to the United States:

> Any property, real or personal, involved in a transaction or attempted transaction in violation of section 1956, 1957 or 1960 of this title, or any property traceable to such property.

6. It is a violation of 18 U.S.C. § 1956(a)(1)(B)(i) (laundering of monetary instruments) to conduct or attempt to conduct a financial transaction 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. It is a violation of 18 U.S.C. § 1956(h) to conspire to engage in the offense of money laundering.

7. Under 18 U.S.C. § 981(a)(1)(A), "[a]ny property, real or personal, involved in a transaction in violation of [18 U.S.C. § 1956], or any property traceable to such property" is subject to forfeiture to the United States. The term "property involved" means tainted and untainted property which has been commingled, so long as the "commingling was done to facilitate money laundering in violation of 18 U.S.C. § 1956(a)(1)(B)(i)." *United States v. McGauley*, 279 F.3d 62, 76 (1st Cir. 2002); *see also United States v. Lyons*, 870 F. Supp. 2d 281, 285-86 (D. Mass. 2012).

CRYPTOCURRENCY BACKGROUND

8. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to-peer, network-based medium of value or exchange that may be used as a substitute for fiat[2] currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrencies are Bitcoin[3] (also known as "BTC"), Litecoin, Monero and Ethereum (also known as "ETH").

9. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object.

10. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued

[2] Fiat currency, such as the U.S. dollar, is backed by a government, but not by a physical commodity such as gold.

[3] Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and "bitcoin" (with a lowercase letter b) to label units of the cryptocurrency. That practice is adopted here.

by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network.

11. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.[4] Cryptocurrency is not illegal in the United States.

12. Ethereum or ETH is a well-known blockchain that can be used to create different cryptocurrencies. There are many Ethereum-based cryptocurrencies that utilize the Ethereum blockchain, which are referred to in the cryptocurrency community as "tokens." Each Ethereum-based token has its own coding (or "smart contract") that governs how the token will operate. Tokens built using the Ethereum blockchain are fungible, meaning they can be exchanged with other Ethereum-based tokens.

13. The TRON network is another well-known blockchain that can be used to create different cryptocurrencies. There are many TRON-based cryptocurrencies that use the TRON blockchain, which are referred to in the cryptocurrency community as "tokens." Each TRON-based token has its own coding (or "smart contract") that governs how the token will operate. Tokens built using the TRON blockchain are fungible, meaning they can be exchanged with other TRON-based tokens.

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

[4] Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

stablecoin. Tether, located in El Salvador, is the company that manages the smart contracts and the treasury (*i.e.*, the funds held in reserve) for USDT tokens.

15. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key.

16. To conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key"). A public address is represented as a case-sensitive string of letters and numbers, 26-40+ characters long, depending on the type of cryptocurrency.

17. Each public address is controlled and/or accessed using a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an address's private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

18. Although cryptocurrencies such as BTC have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes, including money laundering, and is an oft used means of payment for illegal goods and services on hidden services websites operating on the Tor network.

19. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), in an Internet-based cloud storage provider ("online wallet"), on a mobile application on a smartphone

or tablet ("mobile wallet"), through printed public and private keys ("paper wallet"), and in an online account associated with a cryptocurrency exchange. Because these desktop, mobile and online wallets are electronic in nature, they are located on mobile devices (*e.g.*, smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet.

20. Cryptocurrency exchanges are individuals or companies, such as Coinbase a U.S.-based cryptocurrency exchange, that exchange cryptocurrency for other currencies, including U.S. dollars. According to the Department of Treasury, Financial Crimes Enforcement Network ("FinCEN") Guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses.[5] Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law).

21. Registered money transmitters are required by law to follow Bank Secrecy Act ("BSA") anti-money laundering ("AML") regulations, "Know Your Customer" ("KYC") protocols, and other verification procedures similar to those employed by traditional financial institutions. For example, FinCEN registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and the full bank account and routing numbers that the customer links to an exchange account.

BACKGROUND ON CRYPTOCURRENCY INVESTMENT SCHEMES

22. Cryptocurrency investment schemes are schemes in which criminal actors engage

[5] *See* "Application of FinCEN's Regulations to Person Administering, Exchanging, or Using Virtual Currencies," available at https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering.

in social engineering, which allow them to steal victims' funds through virtual currency payments and/or fraudulent investments.

23. Cryptocurrency investment scams typically involve four stages.

a. First, a perpetrator will use a fictious identity and cold-contact a victim, often via text message or messaging application, social media, a dating application, or other communication platform. Oftentimes, the perpetrator will pretend to have contacted the wrong number but will continue communicating with the victim.

b. Second, the perpetrator will establish a relationship and build trust with the victim by continuing to message over days, weeks, or months.

c. Third, the perpetrator will concoct a narrative to induce the victim to send a series of payments in the form of virtual currency. Common narratives include lucrative investment opportunities or emergencies necessitating funds. Many perpetrators will convince victims to use fraudulent websites or applications, controlled by perpetrators to invest in virtual currency. Perpetrators coach victims through the investment process, show them fake profits, and encourage victims to invest more.

d. Fourth, perpetrators disengage victims once they have stolen their funds. In scenarios when victims stop sending more payments, the perpetrator cuts off all contact. In schemes involving fraudulent investment platforms, victims are often told they need to pay a fee or tax when they attempt to withdraw their money. Victims are then unable to get their money back from perpetrators, even if they pay the fake fees or taxes.

FACTUAL ALLEGATOINS

24. As described below, the Defendant Properties were involved in a transactions or attempted transactions in violation of section 18 U.S.C. § 1956(a)(1)(B)(i) (concealment money laundering) and/or 18 U.S.C. § 1956(h) (money laundering conspiracy) or property traceable to such property.

The Online Scam

25. In November 2024, Victim 1, a Massachusetts resident, met a person or persons called "Linda Brown" on an online dating application. After communicating on the dating application, Victim 1 and Brown moved their conversation to Telegram. Brown gained Victim 1's trust by feigning that they could be together in a relationship. For example, Brown sent Victim 1 the following message on Telegram:

> *"If you like it too. When we meet. I can sing it to you. Of course. You can sing it to me too. Maybe I will fall in love with you.lol"*

26. After some time, Brown asked Victim 1 about their finances. For example:

> *"This may be a private question, and you may choose not to answer it, because I'd like to know your annual income."*

27. Eventually, Brown shifted the conversation to cryptocurrency:

> *"Yes Trump's election is definitely good news for us investors, I love discussing this with you, you're a great listener, and if you're also interested in Bitcoin, I can share some of my experiences with you when there are good trading nodes"*

28. After a few weeks, Brown explained she had an investment opportunity for Victim 1 in the cryptocurrency space. Brown directed Victim 1 to the website m.HTFxpro.com ("the website"). Additionally, Brown provided Victim 1 step by step instructions on searching for the Coinbase wallet application and instructed Victim 1 to open Coinbase account, which Victim 1 did. Victim 1 did not have cryptocurrency accounts before engaging with Brown. Victim 1 began with a small investment to build their confidence. Brown walked Victim 1 through the trading

process step-by-step including exchanging screenshots back and forth over Telegram. For example, Brown sent the following messages:

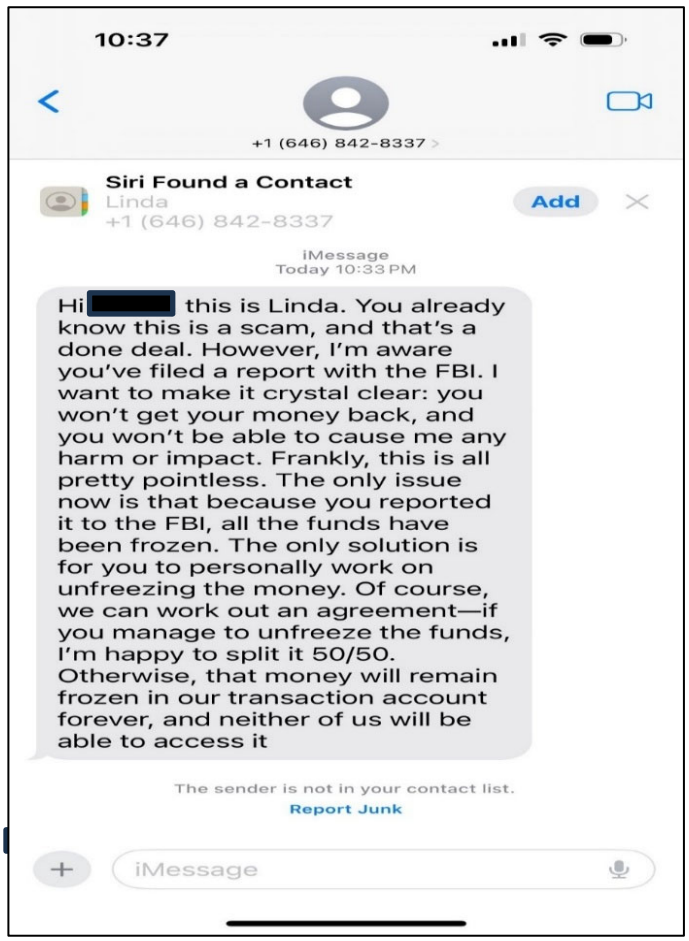
> *"https://m.htfxpro.com*
> *Copy the address and paste it in the search box to open"*
> *...*
> *"Paste the address in the first line and fill in the amount 0.2836 in the second line"*
> *...*
> *"Betting Time: 12:04*
>
> *Buy: Green*
>
> *Buy amount: $350*
>
> *Trading Time: 30 seconds*
>
> *00:03*
>
> *OK?"*

29. Brown warned Victim 1 that they might get a call from the bank where the bank staff would come up with all sorts of excuses to stop Victim 1 from transferring their funds. Brown told Victim 1 to be firm with the bank and reiterate that they have the right to "freely dispose of [their] assets." Brown also instructed Victim 1 to purchase small dollar amounts of various coins on Victim 1's cryptocurrency accounts to "build activity on [their] account, making future transactions smoother and less likely to be flagged."[6]

30. Victim 1 made approximately eight separate transactions from November through late December 2024, totaling approximately $550,000 and which included funds from Victim 1's retirement accounts. Victim 1 was forced to switch financial institutions multiple times to wire funds to legitimate cryptocurrency exchanges because the banks kept preventing additional wire

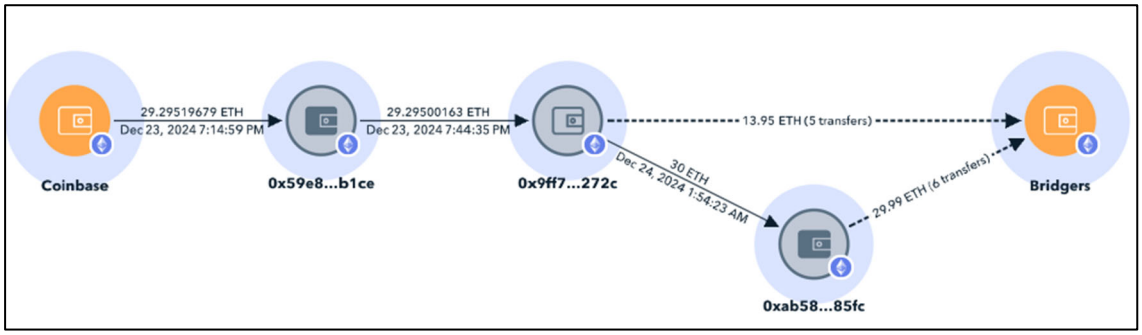
[6] Victim 1 did open legitimate accounts at real cryptocurrency exchanges such as Coinbase and Crypto.com as part of the overall scheme. Victim 1 was instructed to send funds from their cryptocurrency account(s) to wallets controlled by the Target Subjects by using the website m.htfxpro.com contemporaneously with the legitimate cryptocurrency exchange accounts.

transfers. By the end of the scam, the website showed Victim 1 that they had earned a 50% return on their investment, displaying balance of approximately $1.3 million. Victim 1 found out that the investment was a scam when they unsuccessfully attempted to withdraw their money. Victim 1 also read a review online that identified the website as a scam. At one point, Brown informed Victim 1 that they were scammed and asked Victim 1 to personally work on unfreezing the money.



Cryptocurrency Tracing

31. On December 23, 2024, Victim 1 sent approximately 29.29 ETH (~$100,048[7]) on the Ethereum blockchain[8] to an unhosted wallet[9] from their Coinbase account. Victim 1 made this transaction at the direction of Brown. Between December 23, 2024, and December 24, 2024, Victim 1's funds were mingled with other funds and were sent through multiple intermediary unhosted wallets to a bridge, which refers to a mechanism that enables the transfer of digital assets or data between different blockchain networks:



32. On December 24, 2024, the Target Subjects used a bridge to swap the mingled ETH to approximately 103,367 USDT from the Ethereum blockchain to Target Wallet 1 on the TRON Network[10].

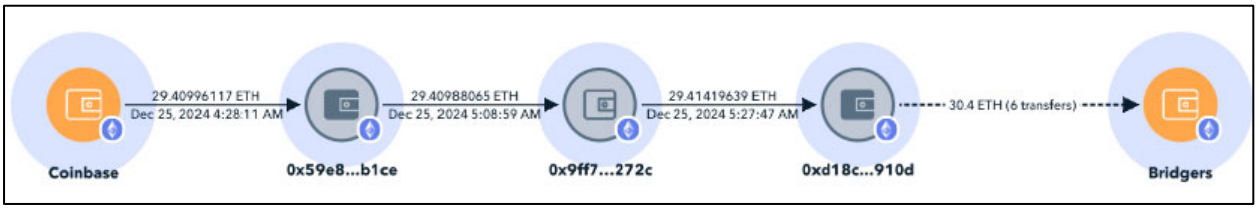
[7] The U.S. dollar amounts discussed r in this section are an estimate based solely upon the historical price of the underlying commodity (*e.g.*, ETH, BTC) on the date of the transaction.

[8] The Ethereum blockchain is denoted by the Ethereum logo at the bottom right of the wallets.

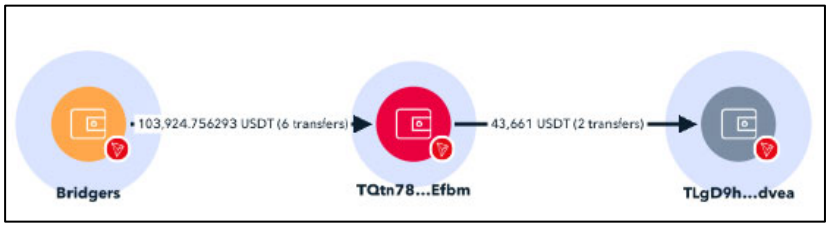
[9] An unhosted wallet, also known as a self-hosted or non-custodial wallet, is a virtual currency wallet through which the user has complete control over storing and securing their private keys and virtual currency. Unhosted wallets do not require a third party's involvement (*e.g.*, a virtual currency exchange) to facilitate a transaction involving the wallet.

[10] The TRON Network is denoted by the TRON logo at the bottom right of the wallets.

33. On December 25, 2024, also at Brown's direction, Victim 1 sent approximately 29.40 ETH (~$102,701) on the Ethereum blockchain to an unhosted wallet from their Coinbase account. Between December 25, 2024, and December 29, 2024, the Target Subjects sent Victim 1's funds through multiple intermediary unhosted wallets to a bridge:



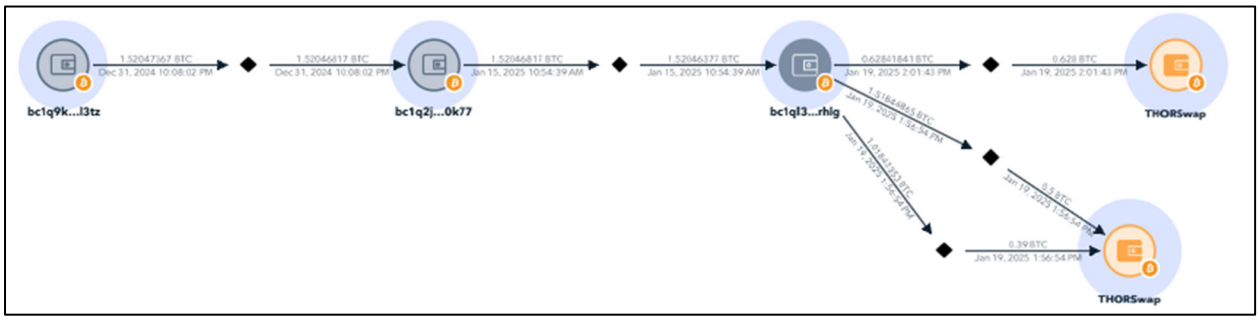
34. On December 29, 2024, the Target Subjects used a bridge to swap the ETH to approximately 103,924 USDT from the Ethereum blockchain to Target Wallet 2 on the TRON Network. On December 30, 2024, Target Wallet 2 sent out approximately 43,661 USDT to an intermediary unhosted wallet:



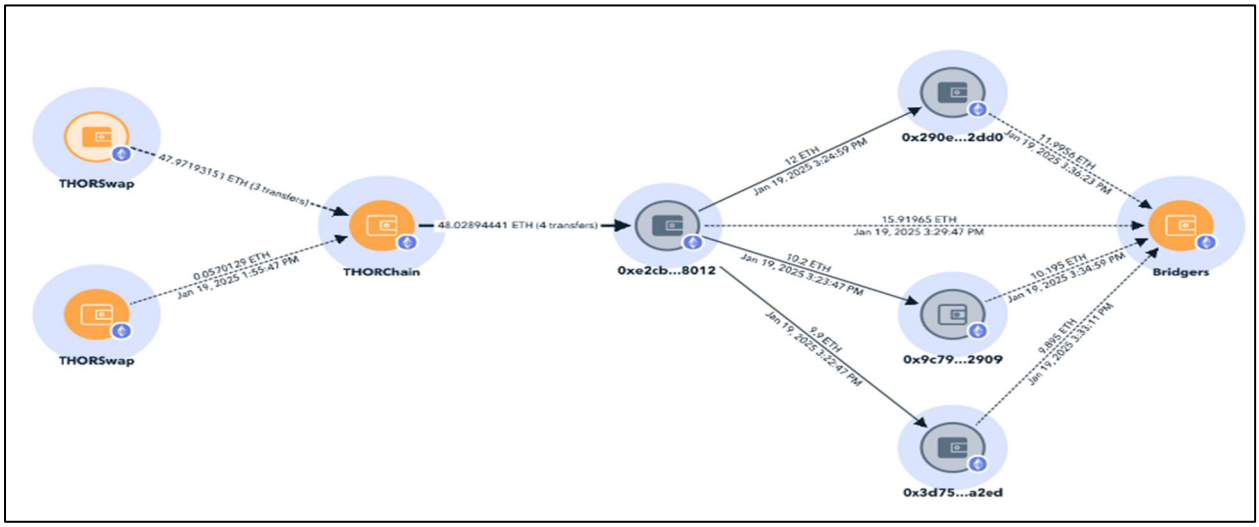
35. On December 31, 2024, at Brown's direction, Victim 1 sent approximately 1.52 BTC (~$142,012) on the Bitcoin blockchain[11] to an unhosted wallet from their account. Between

[11] The Bitcoin blockchain is denoted by the Bitcoin logo at the bottom right of the wallets.

January 15, 2025, and January 19, 2025, the Target Subjects sent Victim 1's funds through multiple intermediary unhosted wallets to a decentralized exchange[12].[13]



36. On January 19, 2025, the Target Subjects utilized a decentralized exchange to swap the BTC to approximately 48.03 ETH (~$154,126) from the Bitcoin blockchain to the Ethereum blockchain and then to an intermediary unhosted wallet. Less than two hours later, Victim 1's funds were sent through multiple intermediary unhosted wallets to a bridge:



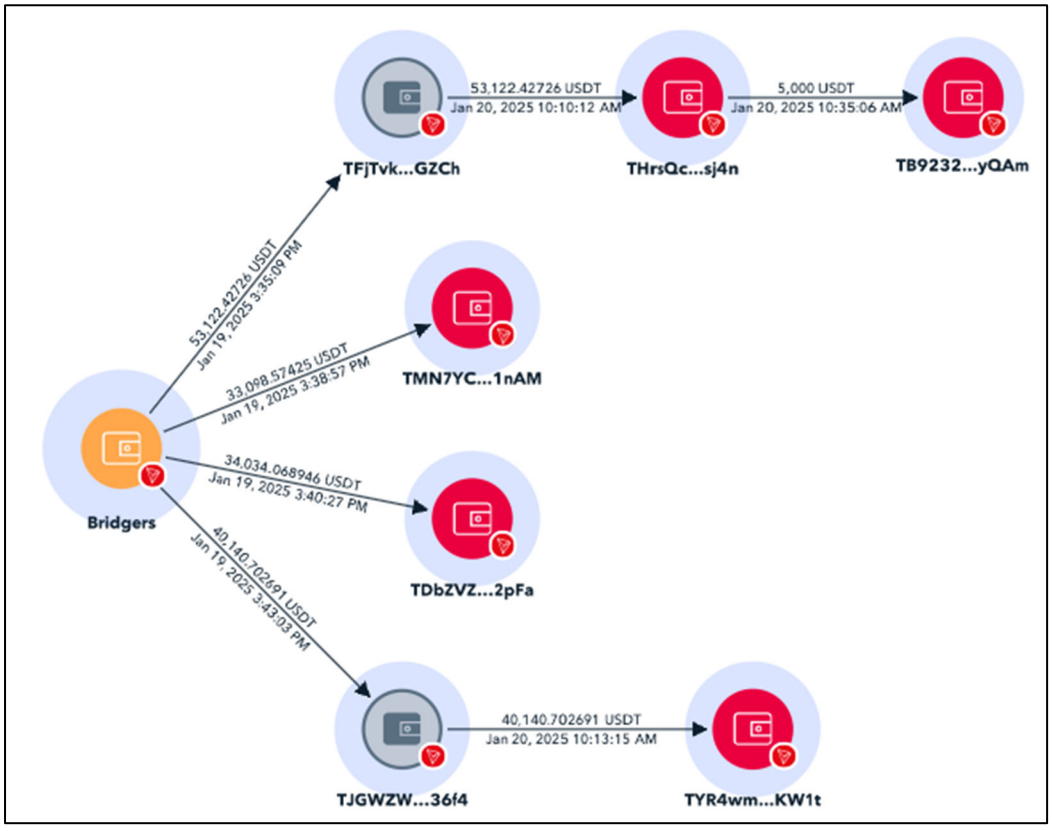
[12] THORSwap is a decentralized exchange (DEX) powered by multi-chain THORChain. THORSwap performs cross-chain swaps in a permissionless, trustless, and non-custodial manner.

[13] Diamond shapes are inserted by tracing software and are not indicative of an additional transfer.

37. On January 19, 2025, the Target Subjects used a bridge to conduct the following transactions, all stemming from the 48.03 ETH:

- Swapped the ETH to approximately 33,098 USDT from the Ethereum blockchain to the Tron Network to Target Wallet 3.
- Swapped the ETH to approximately 34,034 USDT from the Ethereum blockchain to the Tron Network to Target Wallet 4.
- Swapped the ETH to approximately 40,140 USDT from the Ethereum blockchain to an intermediary unhosted wallet on the Tron Network.
- Swapped the ETH to approximately 53,122 USDT from the Ethereum blockchain to another intermediary unhosted wallet on the Tron Network.

38. On January 20, 2025, the Target Subjects sent Victim 1's funds, along with other commingled funds, that had been previously sent to intermediary unhosted wallets to Target Wallet 5, Target Wallet 6, and Target Wallet 7:



39. Based on the foregoing, the 327,829.720952 USDT stored in or on behalf of or associated with the Target Wallets constitutes property involved in a violation of 18 U.S.C. § 1956 (laundering of monetary instruments) and are subject to civil forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(A).

40. The Target Subjects engaged in a scheme to defraud Victim 1 and others of their money and employed material falsehoods to further a scheme to defraud. Specifically, the Target Subjects sent Telegram messages with instructions on how to access a purported trading platform and provided instructions to Victim 1 on how to trade within the platform. Instead of being an actual legitimate investment, the Target Subjects directed Victim 1 to use legitimate cryptocurrency exchanges to send their funds to wallets controlled by the Target Subjects. Instead of investing Victim 1's funds like they promised in the Telegram messages, the Target Subjects converted the BTC/ETH into USDT without Victim 1's knowledge.

41. Money launderers often change the form of cryptocurrency to obscure the source of the funds and make tracing transfers of funds more difficult. They also often used decentralized exchanges that do not do not require Know Your Customer ("KYC") documentation to change the form of cryptocurrency. Money launderers also convert funds to stablecoins such as USDT to avoid market volatility of other forms of cryptocurrency, such as BTC and ETH. Finally, money launderers often use numerous transfers between unhosted wallets to try to obscure the source of the funds and make tracing the transfers of funds more difficult.

42. The tactics displayed by the Target Subjects for transactions containing Victim 1's funds demonstrated tactics and characteristics typically used in money laundering and concealing of the true origin of the victim funds. Specifically, the Target Subjects transferred Victim 1's funds through multiple hops of unhosted wallets, sent Victim 1's funds through multiple chain-swaps,

and converted Victim 1's funds from the original cryptocurrency (BTC/ETH) into a different cryptocurrency (USDT).

CONCLUSION

WHEREFORE, the United States of America requests:

a. That a Warrant and Monition, in the form submitted herewith, be issued to the United States Marshals Service or its designee, commanding seizure of the Defendant Properties, and to give notice to all interested parties to appear and show cause why the forfeiture should not be decreed;

b. That judgment of forfeiture be decreed against the Defendant Properties;

c. That thereafter, the Defendant Properties be disposed of according to law; and

d. For costs and all other relief to which the United States may be entitled.

Respectfully submitted,

LEAH B. FOLEY
United States Attorney

By: /s/ *Annapurna Balakrishna*
Annapurna Balakrishna
Assistant United States Attorney
United States Attorney's Office
1 Courthouse Way, Suite 9200
Boston, Massachusets 02210
(617) 748-3100
annapurna.balakrishna@usdoj.gov

Verification

I, Michael Jankowiak, hereby verify and declare, under penalty of perjury, that I am a Special Agent with the Federal Bureau of Investigation and, pursuant to 28 U.S.C. § 1746, that I have read the foregoing Verified Complaint for Forfeiture *In Rem* and know the contents thereof, and that the matters contained in the Verified Complaint are true to my own knowledge, information, and belief.

The sources of my knowledge and information and the grounds of my belief are the official files and records of the United States, information supplied to me by other law enforcement officers, and my investigation of this case together with other law enforcement officers.

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

Executed this 2nd day of March, 2026

/s/
Michael Jankowiak
Special Agent
Federal Bureau of Investigation