UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. APPROXIMATELY 442,534 USDT FORMERLY ASSOCIATED WITH 0xb1A741CF274d790476e8B9D5c5a377f635BE97CB VIRTUAL CURRENCY ADDRESS, Defendant.	NO. **VERIFIED COMPLAINT FOR FORFEITURE *IN REM***

COMES NOW the United States, by and through its undersigned counsel, and alleges:

I. NATURE OF THE ACTION

1. This is a civil action *in rem*, brought to enforce the provision of 18 U.S.C. § 981(a)(1)(C) for forfeiture of cryptocurrency that constitutes or is derived from proceeds traceable to a violation of specified unlawful activity as defined in 18 U.S.C. § 1956(c)(7), including but not limited to Wire Fraud (18 U.S.C. § 1343) and Conspiracy to Commit Wire Fraud (18 U.S.C. § 1349).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

2. This is a civil action *in rem*, brought to enforce the provision of 18 U.S.C. § 981(a)(1)(A) for forfeiture of cryptocurrency that is involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956 (Money Laundering and Conspiracy to Commit Money Laundering), or any property traceable to such property.

II. PLAINTIFF AND DEFENDANT *IN REM*

3. The plaintiff is the United States of America (the "Plaintiff" or "Government" or "United States").

4. The defendant consists of approximately 442,534 USDT (the "Defendant Cryptocurrency"), formerly associated with virtual currency address 0xb1A741CF274d790476e8B9D5c5a377f635BE97CB (the "Subject Address"), seized by the Federal Bureau of Investigation ("FBI") on or about June 4, 2026.

5. The Subject Address was associated with an unhosted wallet that contained USDT tokens. The USDT tokens were managed by Tether International S.A. de C.V. ("Tether").

6. Pursuant to a forfeiture seizure warrant issued in the Western District of Washington, Cause No. MC26-011, and executed on or about February 20, 2026, Tether re-issued the USDT and transferred it to a government-controlled wallet. The United States took custody of the Defendant Cryptocurrency on or about June 4, 2026. The Defendant Cryptocurrency is currently in the custody of the United States Marshals Service.

7. According to www.etherscan.io, when the Defendant Cryptocurrency was transferred to the United States on or about June 4, 2026, it was valued at approximately $442,505.68.

III. JURISDICTION AND VENUE

8. This Court has jurisdiction over an action commenced by the United States under 28 U.S.C. § 1345 and has jurisdiction over an action for forfeiture under 28 U.S.C. §§ 1355(a) and (b).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

9. Venue is proper in this district pursuant to 28 U.S.C. § 1355(b)(1)(A) because the acts or omissions giving rise to the forfeiture occurred in this district.

10. Pursuant to 18 U.S.C. § 981(f), all right, title, and interest in the Defendant Cryptocurrency vests in the United States at the time of the acts giving rise to the forfeiture.

11. Pursuant to Supplemental Rule G(2)(f), facts in support of a reasonable belief that the United States will be able to meet its burden of proof at trial are as follows and have been verified by the attached Verification of FBI Special Agent Andrew Cropcho.

12. As provided in Supplemental Rule G(3)(b)(i), the Clerk of Court is required to issue a warrant to arrest the Defendant Cryptocurrency if it is in the government's possession, custody, or control. As such, the Court will have *in rem* jurisdiction over the Defendant Cryptocurrency when the accompanying Warrant of Arrest *In Rem* is issued, executed, and returned to the Court.

IV. SUMMARY OF BASES FOR FORFEITURE

13. The United States alleges that the Defendant Cryptocurrency was involved in transactions and attempted transactions in violation of 18 U.S.C. § 1956 (Money Laundering and Conspiracy to Commit Money Laundering) and constitutes, or was derived from, proceeds traceable to violations of 18 U.S.C. §§ 1343 (Wire Fraud) and 1349 (Conspiracy to Commit Wire Fraud). The Defendant Cryptocurrency is, therefore, subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and (a)(1)(C).

14. The Defendant Cryptocurrency contains funds swindled from victims, including victims in the Western District of Washington, through the course of a work-from-home scheme, which is described in more detail herein. These funds were subsequently laundered through a series of cryptocurrency addresses and cryptocurrency "swaps" before coming to rest in the Subject Address. Ultimately, though the funds were

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

defrauded from multiple victims and traveled different paths, they arrived at the same destination.

15. As part of the scheme, victims were engaged by someone online about a work-from-home opportunity to make money. In connection with the purported opportunity, victims were instructed how to perform certain tasks. After completing a certain number of tasks, funds accumulated in their supposed accounts.

16. To gain access to more tasks, the victims were instructed to send virtual currency to addresses associated with the fraudsters. However, after the victims accumulated supposed income by completing tasks, they were ultimately unable to withdraw the balance in their accounts, and they were also unable to withdraw their own funds that they sent to the fraudsters to unlock tasks to perform. Eventually, the fraudsters ceased contact with the victims, who lost all of the funds they sent to the fraudsters.

17. The perpetrators of the wire fraud scheme used multiple techniques to facilitate the fraud and to conceal and disguise the source and destination of the illicitly procured funds. They instructed victims to transfer funds to multiple virtual currency addresses that they controlled, then rapidly moved the funds from the original gaining addresses to other addresses they controlled. They used multiple virtual currency exchange accounts, conducted cryptocurrency "swaps" (such as from Ethereum to USDT), and comingled funds defrauded from multiple victims with other funds to further conceal and disguise the fraud proceeds.

18. Using the Lowest Intermediate Balance Rule ("LIBR") tracing methodology, law enforcement traced approximately $62,179 in funds defrauded from victims of the work-from-home scheme to the Subject Address. The proceeds traced to the Subject Address are forfeitable as proceeds of the underlying wire fraud and wire fraud conspiracy. The remaining USDT in the Subject Address is forfeitable as property involved in money laundering and money laundering conspiracy, as set forth herein.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

19. On or about February 20, 2026, the FBI executed a properly authorized federal search warrant for the USDT associated with the Subject Address.

20. On or about June 4, 2026, approximately 442,534 USDT was reissued into a virtual currency wallet under control of the United States.

V. PURPOSE OF FORFEITURE

21. The purpose of this forfeiture action *in rem* is two-fold. First, forfeiture of the Defendant Cryptocurrency provides a means for the United States to help victims of the fraud scheme recover their funds. Second, forfeiture deters criminal activity by forfeiting and vesting title of the Defendant Cryptocurrency with the United States so that criminals do not maintain the fruits of crime and do not keep property that facilitated or was involved in crime.

VI. THE LAW

22. Pursuant to 18 U.S.C. § 1343, it is unlawful to devise or intend "to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, 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. . . ."

23. Pursuant to 18 U.S.C. § 1349, it is unlawful to attempt or conspire to commit a violation of 18 U.S.C. § 1343.

24. Pursuant to 18 U.S.C. § 981(a)(1)(A), "[a]ny property, real or personal, involved in a transaction or attempted transaction in violation of [a federal money laundering offense, 18 U.S.C. § 1956], or any property traceable to such property" is subject to forfeiture to the United States.

25. Pursuant to 18 U.S.C. § 981(a)(1)(C), "[a]ny property, real or personal, which constitutes or is derived from proceeds traceable to a violation of . . . any offense

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

constituting a 'specified unlawful activity' (as defined in section 1956(c)(7) of this title), or a conspiracy to commit such offense" is subject to forfeiture to the United States.

26. Pursuant to 18 U.S.C. § 1956(a)(1), it is unlawful to knowingly conduct or attempt to conduct a "financial transaction" with proceeds from "specified unlawful activity" ("SUA") with specific intent to: promote the SUA, conceal or disguise the source, origin, nature, ownership, or control of the proceeds, evade reporting requirements, or evade taxes.

27. Pursuant to 18 U.S.C. § 1956(h), it is also unlawful to conspire to commit a money laundering offense.

28. Pursuant to 18 U.S.C. § 1956(c)(7) and 18 U.S.C. § 1961(1)(B), the offenses of wire fraud and conspiracy to commit wire fraud, in violation of 18 U.S.C. §§ 1343 and 1349, constitute specified unlawful activity.

VII. BACKGROUND ON DIGITAL OR VIRTUAL CURRENCY

29. Virtual or Digital Currency: Digital currency (also known as cryptocurrency or virtual currency)[1] is generally defined as an electronic-source unit of value that can be used as a substitute for fiat currency (i.e., currency created and regulated by a government). 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 currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies.[2] Digital currency is not issued by any government or bank (in contrast to fiat currency) and is, instead, generated and controlled through computer software operating on a decentralized peer-to-peer network. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud based servers.

[1] For purposes of this Complaint, the terms "digital currency," "cryptocurrency," and "virtual currency" are used interchangeably and address the same concept.

[2] Fiat currency is currency issued and regulated by a government, such as the U.S. Dollar, Euro, or Japanese Yen.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

30. Digital currency is legal in the United States and accepted for legitimate financial transactions. However, it is also often used for conducting illegal transactions or for concealing or disguising the true nature, source, location, ownership, or control of illegally obtained criminal proceeds. Bitcoin ("BTC") and Ethereum ("ETH") are some of the most commonly used and well-known digital currencies.

31. Stablecoins: 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. For example, USDT is a stablecoin pegged to the U.S. dollar. Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives.

32. Tether: Tether International S.A. de C.V. ("Tether") is the company that manages the smart contracts and the treasury (i.e., the funds held in reserve) for USDT tokens. Tether does not host wallets or virtual currency addresses.

33. Perpetrators of fraud will often conduct an otherwise unnecessary number of transactions in the transfer of funds in an effort to layer ill-gotten funds to ultimately conceal or disguise the nature, location, source, ownership, or control of those proceeds when transferred into a cryptocurrency exchange. The number of hops in the transactions is a strong indication that the movement of funds was performed in a manner meant to conceal or disguise the nature, location, source, ownership, or control of the proceeds of a specified unlawful activity, to wit, wire fraud.

34. Perpetrators of fraud often launder proceeds of their fraud schemes through several virtual wallet addresses or accounts before transferring the proceeds to those individuals near or at the top of the criminal organization's hierarchy.

35. Virtual or Digital Currency Addresses: Digital or virtual currency addresses are the specific virtual locations to which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a strong of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

alphanumeric characters. A user of virtual currency can utilize multiple addresses at any given time and there is no limit to the number of addresses any one user can utilize.

36. Private Key: Each virtual currency address is controlled through a unique corresponding private key, a cryptographic equivalent of a password needed to access the address. Only the holder of an address's private key can authorize a transfer of virtual currency from that address to another address.

37. Address Owner: The identity of an address owner is generally considered to pseudonymous (unless the owner opts to make the information publicly available), often law enforcement and currency exchanges can use the blockchain to identify the owner of a particular address and trace fraud proceeds from victims to one or more exchanges or wallets. The analysis can also, in some instances, reveal additional addresses controlled by the same individual or entity.

38. Virtual currency wallet: There are various types of virtual currency wallets, including software wallets, hardware wallets, paper wallets. A software wallet is a software application that interfaces with the virtual currency's specific blockchain and generates and stores a user's addresses and private keys. A virtual currency wallet allows users to store, send, and receive virtual currencies. A virtual currency wallet can hold many virtual currency addresses at the same time.

39. Hosted and Unhosted Wallets: Wallets that are hosted by third parties are referred to as "hosted wallets" because the third party retains a customer's funds until the customer is ready to transact with those funds. Conversely, wallets that allow users to exercise total, independent control over their funds are often called "unhosted" wallets.

40. Blockchain: The code behind many virtual currencies requires that all transactions involving that virtual currency be publicly recorded on what is known as a blockchain. The blockchain is essentially a distributed public ledger, run by a decentralized network of computers and using that blockchain's technology, containing an immutable and historical record of every transaction. The blockchain can be updated

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

multiple times per hour and records every virtual currency address that has ever received that 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.

41. Blockchain explorer: Blockchain explorers are online tools that operate as a blockchain search engine. Blockchain explorers enable users to search for and review transactional data for any addresses on a particular blockchain. A blockchain explorer is software that uses API and blockchain nodes to draw data from a blockchain and uses a database to arrange and present the data to a user in a searchable format.

42. Ethereum: Ethereum ("Ether" or "ETH") is a cryptocurrency that is open-source and is distributed on a platform that uses "smart contract" technology. Transactions involving ETH are publicly recorded on the Ethereum blockchain, which allows anyone to track the movement of ETH.

43. Virtual Currency Exchange: Virtual currency exchanges ("VCEs") are trading and/or storage platforms for virtual currencies such as BTC and ETH. Many VCEs also store their customers' virtual currency in virtual currency wallets. As previously stated, these wallets can hold multiple virtual currency addresses. Because VCEs act as money services businesses, they are legally required to conduct due diligence of their customers (i.e., "know your customer" or "KYC" checks) and to have anti-money laundering programs in place.

44. Blockchain analysis: It is virtually impossible to look at a single transaction on a blockchain and immediately ascertain the identity of the individual behind the transaction. That is because blockchain data generally consist only of alphanumeric strings and timestamps. But law enforcement can obtain leads regarding the identity of the owner of an address by analyzing blockchain data to figure out whether that same individual is connected to other relevant addresses on the blockchain. To analyze blockchain data, law enforcement can use blockchain explorers as well as commercial

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

services offered by several different blockchain-analysis companies. These companies analyze virtual currency blockchains and attempt to identify the individuals or groups involved in transactions. For example, when an organization creates multiple [BTC] addresses, it will often combine its [BTC] addresses into a separate, central [BTC] address (i.e., a "cluster"). It is possible to identify a 'cluster' of [BTC] addresses held by one organization by analyzing the [BTC] blockchain's transaction history. Open-source tools and private software products can be used to analyze a transaction." *United States v. Gratkowski*, 964 F.3d 307, 309 (5th Cir. 2020). Through numerous unrelated investigations, law enforcement has found the information provided by these tools to be reliable.

VIII. SCHEME TO DEFRAUD AND FINANCIAL TRACING

45. This case involves a work-from-home fraud scheme, perpetrated on victims across the United States, including in the Western District of Washington. After defrauding funds from their victims, the perpetrators engaged in layered financial transactions designed, in whole or in part, to conceal and disguise the nature, location, source, ownership, or control of the proceeds. Proceeds defrauded from at least three identified victims of the wire fraud scheme flowed into and through virtual currency addresses controlled by the perpetrators. Funds from two of the three identified victims were ultimately traced to the Subject Address, where they were seized.

Victim 1, V.M.

46. Victim 1 [V.M.] resides in the Western District of Washington. Around December 2025, V.M. was approached by someone online purporting to be a recruiter for a company named IAMOTA. The recruiter offered V.M. an opportunity to earn commissions by rating products on IAMOTA's platform, https://504593.iamota-reviews.cyou. At first, V.M. was able to withdraw small profits, so she believed that the opportunity was legitimate.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

47. V.M. was convinced to upgrade to higher "VIP" levels to withdraw her earnings, which required V.M. to make deposits into her IAMOTA account. V.M. used Coinbase to transfer at least $200,000 worth of ether to IAMOTA to upgrade her account. Over time, restrictions were added to V.M.'s account, which required continued deposits of her own funds. However, V.M. was never able to make withdrawals. Eventually, V.M. became suspicious of IAMOTA so she contacted the CEO of the real IAMOTA company, which was when V.M. learned that she had fallen for a scam being operated by at least one fraudster impersonating IAMOTA.

48. V.M. provided records for ether transfers that she made at the direction of the IAMOTA impersonator. The transfers happened between about December 8, 2025, through about December 21, 2025, and consisted of about 64 ether, worth approximately $198,000 at the time of transfer.

49. V.M. sent about 89% of the funds to 0x8efc64e5e55444a13055296472194a750013a927 (0x8efc64) in about 9 transactions, comprising a total of about 57 ether. Most times, after V.M. made a deposit into 0x8efc64 it was very soon after transferred to a different address.

50. On about December 17, 2025, when the balance in 0x8efc64 was about 0 ether, V.M. transferred about 16.9 ether to 0x8efc64. About one minute later, approximately 16.87 ether was transferred from 0x8efc64 to 0xa5593244a72a0424610fd4a1355937c6280640ef (0xa55932), and about 36 minutes after the first transfer, the remaining 0.03 ether was also transferred to 0xa55932.

51. 0xa55932 received only one additional deposit, which was a deposit of about 0.37 ether transferred by V.M., on about December 17, 2025. Less than six hours later, on about December 18, 2025, 17.27 ether, the entire contents of the address were transferred from 0xa55932 to 0x1e325e192b4ce3a933fb9dcaf38f92f28334c10e (0x1e325e), an address into which funds from another victim, T.A., were deposited.

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Victim 2, T.A.

52. T.A., a resident of Texas, reported to the FBI that she lost approximately $147,000 as a result of a work-from-home scheme named FriendBuy. According to T.A., starting in about July 2025, she was convinced that she could earn money on a platform called FriendBuy, where she was taught how to promote merchandise online. By promoting specific items, T.A. believed she earned 1% of the sales price. T.A. promoted something by clicking on it using the FriendBuy platform.

53. Over time, as T.A. continued to promote items, she was required to deposit her own funds to get more expensive packages to promote. The more T.A. deposited, the bigger package she was able to get. T.A. was promised that she would have her funds returned to her.

54. Initially, T.A. used her Coinbase account to transfer funds to FriendBuy. However, Coinbase started to scrutinize these transactions, so FriendBuy personnel instructed T.A. to create a virtual currency account at MetaMask. MetaMask is an unhosted wallet, so there was no oversight by a compliance team, and therefore no one to scrutinize T.A.'s transactions. At the direction of FriendBuy, T.A. first sent funds from her Coinbase account to her MetaMask account, and then she used her MetaMask account to send funds to FriendBuy.

55. T.A. became concerned about withdrawing her funds, so she submitted a complaint on the "Cyber complaints" section of a different platform she knew of. After submitting the complaint, T.A. was added to a WhatsApp group called "Billionaire Energy A3F." The members in Billionaire Energy were supportive of T.A. and showed her screenshots of the withdrawals that they were supposedly able to make. Due to her renewed confidence in FriendBuy, T.A. decided to put more of her own funds into the platform.

56. Eventually, around December 17, 2025, T.A. finished her promotions and attempted to withdraw her funds. FriendBuy's finance department told T.A. that she

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

needed to pay 20% of the final withdrawal amount as insurance. T.A. has been unable to withdraw her funds from the FriendBuy platform, and the Billionaire Energy WhatsApp group has blocked her.

57. T.A. paid FriendBuy using ether and USDT. At least two of the ether transfers from T.A. were commingled with V.M.'s ether.

58. Records provided by T.A. show that a 5.68 ether transfer was sent on December 17, 2025, to 0x2adeafe3ba6a42fdebdb1f956142d041db34a185 (0x2adeaf). At the time of the transfer, the balance in 0x2adeaf was about 0.67 ether. About three hours later, a second transfer of 0.32 ether was sent by T.A., which was traced to 0x2adeaf, and about six hours later the entire balance of 0x2adeaf, 6.67 ether, was transferred from 0x2adeaf to 0x1e325e. T.A.'s funds comprised about 90% of the ether that was transferred.

Consolidation 1

59. The ether traceable to T.A. was deposited in 0x1e325e about one minute after the ether traceable to V.M was deposited in 0x1e325e, and all of the transfers described above occurred in less than 10 hours.

60. The 23.94 ether containing funds from V.M. and T.A. were commingled with about 10.29 ether in 0x1e325e. On about December 18, 2025, about 33.8 ether was transferred from 0x1e325e to 0x226dff9f8e259a45c5c1a1cea75db93b9eff7429 (0x226dff). At this time, a balance of 0.44 ether remained in 0x1e325e, all of which is traceable to V.M. and T.A., and eventually combined with funds from another victim, F.Z., discussed in the following section.

61. The 33.8 ether was the only ether deposit into 0x226dff, all of which was transferred from 0x226dff to 0xe12249fd3a015820b6eb9e7704eda78ded4c6078 (0xe12249) about 90 minutes later.

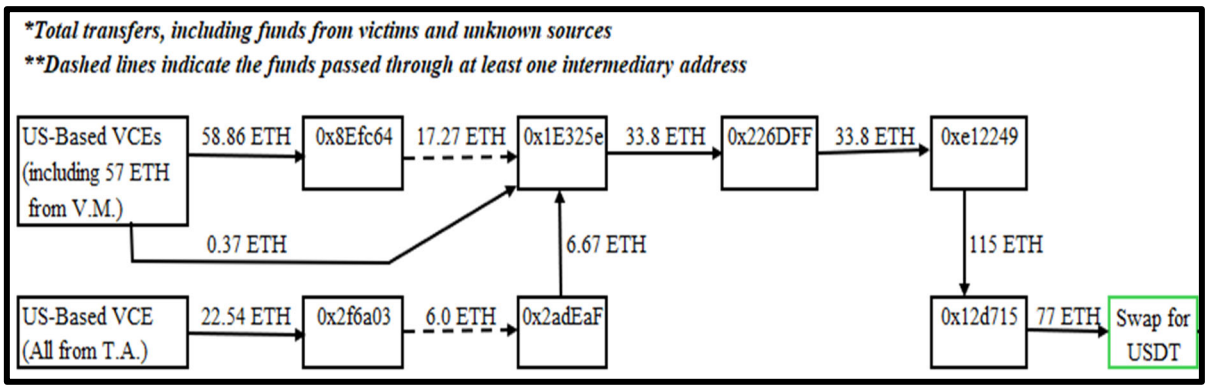
62. The first ether deposit into 0xe12249 happened on about December 16, 2025, and, over about two days, 0xe12249 received a total of eight deposits of ether,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

including the 33.8 ether described in the preceding paragraph; there were no transfers out during this time. After the eighth deposit, the balance in 0xe12249 was about 77.58 ether, and, approximately 12 minutes later, 77 ether was transferred from 0xe12249 to 0x12d7157fc373a938032cd69d8e9ab1bba15abcf9 (0x12d715). This transfer comprised about 22.26 ether (about 29%) that is traceable to V.M. and T.A. using LIBR.

63. On about December 18, 2025, using a decentralized exchange, the 77 ether were swapped for about 227,011 USDT in two transactions, which were the first two transfers of USDT into 0x12d715. The next transaction was an additional deposit of about 20,240 USDT. All of the deposits happened within about three minutes of each other.

64. The series of transactions described above are depicted below:



65. The next five USDT transactions involving 0x12d715 happened on December 18, 2025. The five transactions were withdrawals in batches of approximately 50,000 USDT, all of which happened within about 35 minutes of each other. Each of these withdrawals went to a different anonymous account at a VCE named Poloniex. The accounts were registered using an anonymous email service provided by Proton, and they did not have names associated with them.

66. After each Poloniex account received the aforementioned deposit, about the same amount was transferred to 0xc8b5448353255176faa29dad3fd21429c97b5296 (0xc8b544). At the time of each deposit, the corresponding Poloniex account had

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

approximately no funds in its balance. In total, about 247,252 USDT was transferred to the Poloniex accounts from 0x12d715, and about 247,227 USDT was transferred from the Poloniex accounts to 0xc8b544. These five transfers were the first USDT deposits into 0xc8b544, two of which contained a total of about 26% of funds traceable to V.M. and T.A.

67. On December 18, 2025, about one minute after the fifth transfer from Poloniex, about 243,790 USDT was transferred from 0xc8b544 to 0xb1a741cf274d790476e8b9d5c5a377f635be97cb (the Subject Address). This was the first deposit of USDT into the Subject Address. Between about December 19, 2025, and January 14, 2026, the Subject Address subsequently received three additional deposits comprised of about 503,617 USDT. On about January 29, 2026, approximately 304,873 USDT was transferred out of the Subject Address; there were no further deposits or withdrawals before execution of the forfeiture seizure warrant. When the warrant was executed on or about February 20, 2026, the balance of the Subject Address was approximately 442,534 USDT, of which approximately 62,179 USDT (14%) is traceable to V.M. and T.A.

//

//

//

//

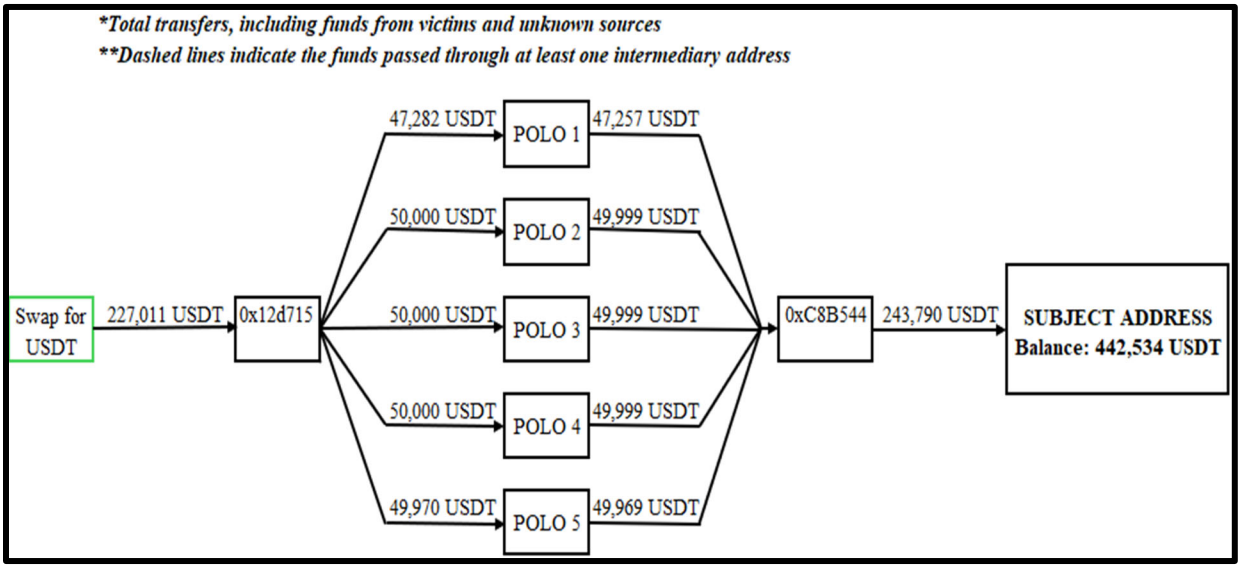
//

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

68. The series of transactions described above, starting at the swap of USDT until the deposit in the Subject Address, is depicted below[3]:



69. The remaining funds in 0xc8b544 were transferred to deposit address 0x75c6b0ca949abc77d0bd154b3ccb985e1c84d3b6 (0x75c6b0) at KCEX.com, a VCE. This matches a similar series of transactions involving a third victim, F.Z., which is described in the next section.

Victim 3, F.Z.

70. According to F.Z., around November 4, 2025, she was contacted online by a representative of a company called ScaleBay. F.Z. was offered a remote job that would help her to earn $200 – $300, per day. In the beginning, F.Z. was about to make two withdrawals, totaling $330; however, ScaleBay made it difficult to make withdrawals. ScaleBay kept demanding that F.Z. deposit more of her own funds to advance to the next

//

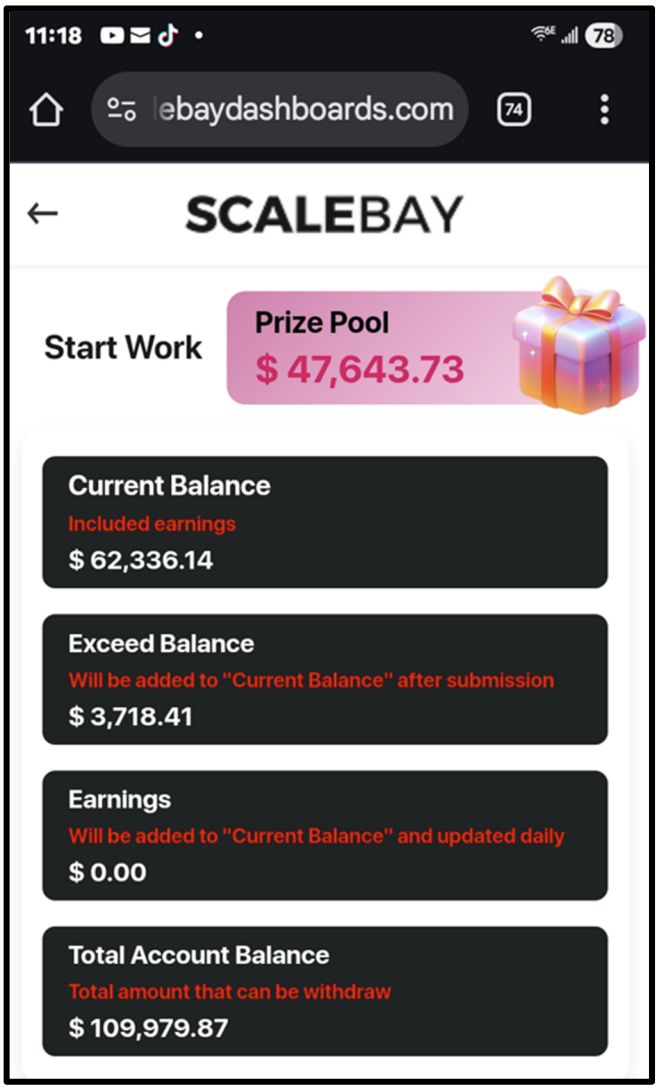
//

//

[3] "POLO" represents a Poloniex account.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

stage, with the claim that she would eventually be able to withdraw her funds. A photo of part of the ScaleBay interface is provided below:



71. Near the end of her interactions with ScaleBay, F.Z. received notice that her funds were intercepted on the blockchain and she needed to pay 9% of the value of the funds to get her money back. At this point, F.Z. realized that ScaleBay was attempting to get more of her funds, and that she had lost her life savings and funds she had borrowed from others, amounting to a total of about $40,000.

72. F.Z. made payments to ScaleBay in bitcoin and ether.

73. On about December 18, 2025, F.Z. transferred about 0.68 ether into 0x239db3dbb497396c390f0d994eba6d20ba047c71 (0x239db3), where it was

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

commingled with about 2.79 ether and transferred to 0x1e325e, where funds from V.M. and T.A. were previously transferred.

74. 0x1e325e had an existing balance of about 15.47 ether, about 0.12 of which were traceable to V.M. and T.A. based on LIBR tracing methodology, at the time 0x1e325e received the transfer of funds, which included funds from F.Z.

75. On December 19, 2025, and about 30 minutes after F.Z.'s funds were transferred to 0x1e325e, 18.5 ether was transferred from 0x1e325e to 0xc0e75c8bdaa39cbc10168dc46c265f6d16fbc28a (0xc0e75c); this was about 98% of the balance of 0x1e325e at this time.

76. The 18.5 ether transferred to 0xc0e75c was its only deposit, and about 13 minutes later the entire balance of 18.5 ether, which included about 0.36 ether traceable to V.M., T.A., and F.Z., was transferred to 0xe12249, which is the same address the flow of funds from V.M. and T.A. travelled before being swapped for USDT.

77. 0xe12249 had a balance of about 20.8 ether before it received the 18.5 ether from 0xc0e75c. On December 19, 2025, about 38 ether (about 98% of 0xe12249's balance) was transferred to 0x12d715, continuing on the same route as the first set of transfers described in the previous section.

//

//

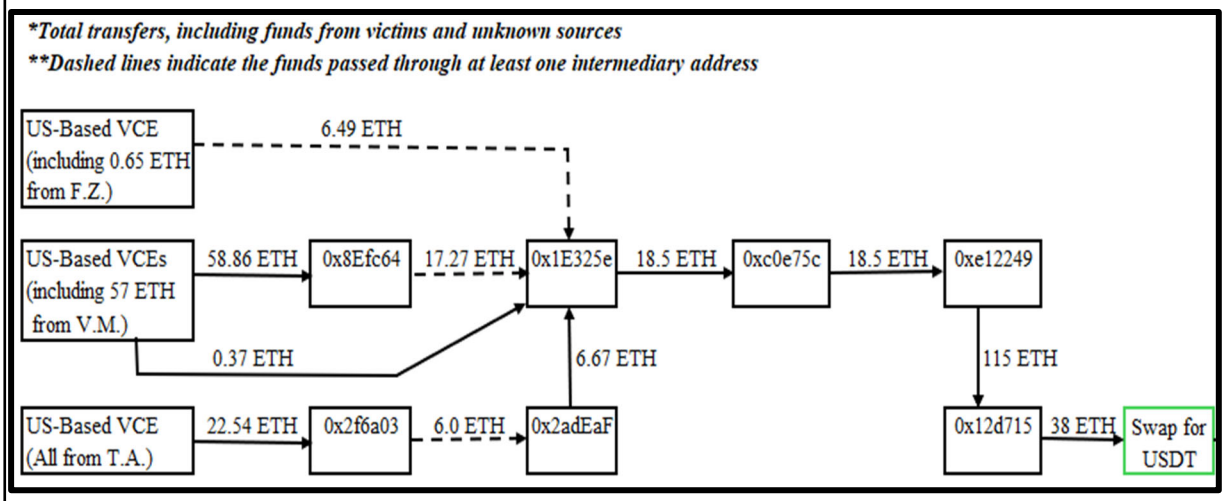
//

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

78. The deposit of 38 ether was the second deposit into 0x12d715. A depiction of the transfers described above is provided below:



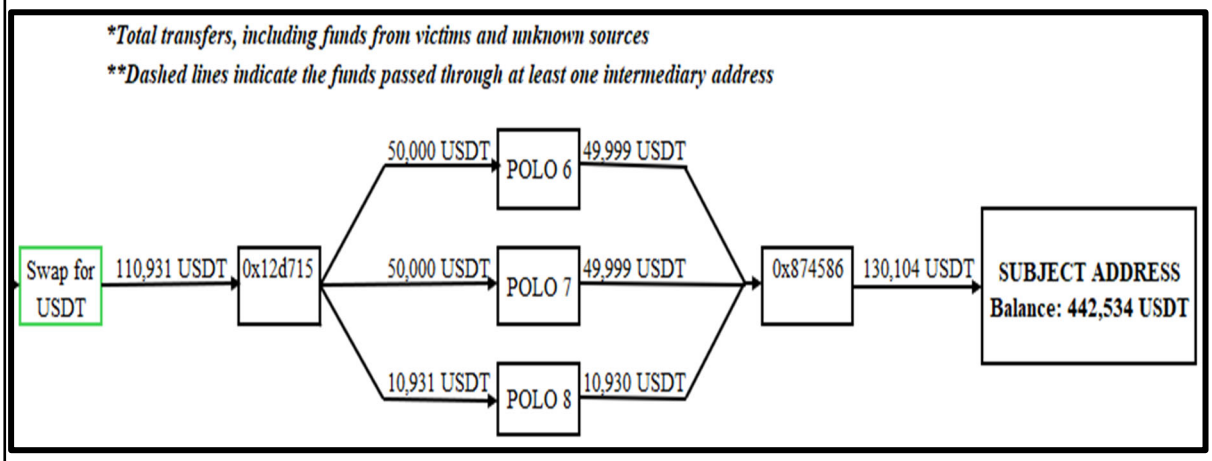
79. Shortly after the 38 ether was deposited, a decentralized exchange was used to swap about 37.99 ether for about 110,931 USDT. About 0.01 ether remained in 0x12d715 after the swap.

80. Within about three minutes of receiving the 110,931 USDT, 0x12d715 made three transfers to three different accounts at Poloniex, which were also registered without names and using an anonymous email service provided by Proton. Three transfers happened in two increments of 50,000 USDT and one increment of 10,931 USDT, which was about the entirety of the balance in 0x12d715. Based on LIBR tracing methodology, the 10,931 USDT contained about 1,034 USDT of victim funds.

81. On December 19, 2025, within about 15 minutes of receiving the transfers from 0x12d715, each Poloniex account transferred about the same amount of USDT it received to 0x87458645d10385beafba4afdf1868b1ce9a39fe5 (0x874586). This total of about 110,929 USDT was combined with one additional transfer of 20,782 USDT and constituted the only four USDT deposits into 0x874586 at this time. Besides one subsequent deposit of 0.01 USDT, the next USDT transaction in 0x874586 was a transfer of about 130,104 USDT to the Subject Address. Based on LIBR tracing methodology, no victim funds were contained in this transfer.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

82. The series of transactions described above, from the swap of USDT to the Subject Address, are depicted below:



83. After this transfer, there was about 1,607 USDT remaining in 0x874586, which contained about 1,034 USDT of victim funds. The 1,607 USDT was transferred to deposit address 0x75C6B0 at the KCEX.com VCE, which is the same destination as the remaining USDT left in the penultimate address described in the first section.

84. Although no known victim funds in this second series of transactions are traceable to the Subject Address, the similar modus operandi shows that all three victims likely fell victim to the same fraud actor or group of fraud actors who control the addresses, including the Subject Address, described above in the work-from-home fraud schemes. This supports a reasonable belief that the USDT held in the Subject Address represents proceeds of wire fraud and property involved in money laundering.

85. Using the Lowest Intermediate Balance Rule ("LIBR") tracing methodology, law enforcement traced approximately 62,179 USDT that was defrauded from victims of the work-from-home fraud scheme to the Subject Address. In light of the additional victim reports connected to tracing of funds through the blockchain into addresses that also funneled into the Subject Address, there is reasonable cause to believe that a greater amount of funds in the Subject Address constituted not only proceeds of the underlying wire fraud scheme but also property involved in money laundering

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

transactions, such that all of the USDT formerly associated with the Subject Address is subject to forfeiture.

86. The perpetrators of the wire fraud scheme used multiple techniques to facilitate the fraud and to conceal and disguise the source and destination of the illicitly procured funds. They instructed victims to transfer funds to multiple virtual currency addresses that they controlled, then rapidly moved the funds from the original gaining addresses to other addresses they controlled. They used multiple virtual currency exchanges, conducted cryptocurrency "swaps" (such as from Ethereum to USDT), and comingled funds defrauded from multiple victims with other funds to further conceal and disguise the fraud proceeds.

IX. CLAIM FOR RELIEF

87. As required by Supplemental Rule G(2)(f), the facts set forth in this Verified Complaint support a reasonable belief that the United States will be able to meet its burden of proof at trial. More specifically, there is probable cause to believe that the Defendant Cryptocurrency is forfeitable pursuant to 18 U.S.C. § 981(a)(1)(C) because it constitutes or is derived from proceeds of Wire Fraud, in violation of 18 U.S.C. § 1343 and Conspiracy to Commit Wire Fraud, in violation of 18 U.S.C. § 1349, and pursuant to 18 U.S.C. § 981(a)(1)(A) because it is property involved in Money Laundering and Conspiracy to Commit Money Laundering, in violation of 18 U.S.C. § 1956.

//

//

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

WHEREFORE, the United States respectfully requests:

1. A warrant be issued for the arrest of the Defendant Cryptocurrency;
2. Due notice be given to all interested parties to appear and show cause why the Defendant Cryptocurrency should not be forfeited;
3. Judgment be entered declaring the Defendant Cryptocurrency, any derivative cryptocurrency, and any interest to be condemned and forfeited to the United States for disposition according to law; and,
4. The United States be granted such other and further relief as this Court may deem just and proper.

DATED this 9th day of October, 2026.

KRISTA K. BUSH
Assistant United States Attorney
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, Washington 98101
Phone: (206) 553-2242
Fax: (206) 553-6934
Krista.Bush@usdoj.gov

VERIFICATION

I, Andrew Cropcho, I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") and have been so employed since May 2018. I am currently assigned to the Seattle Field Office.

My primary duties as an FBI Special Agent include investigating violations of federal law, including financial fraud, corporate fraud, securities fraud, government program fraud, and healthcare fraud. Part of those duties include investigating instances of wire fraud being used for financial gain at the expense of others, which has involved examining financial accounts and obtaining and reviewing data from warrants for electronic devices and online accounts, including social media, cloud storage, and e-mail accounts. Before my career as an FBI Special Agent, I was employed at a large public accounting firm for over three years and, as part of my employment, I examined financial information of clients to determine their accuracy, reliability, and sources.

In the scope of my duties as an FBI Special Agent, within the meaning of Rule 41(a) of the Federal Rules of Criminal Procedure, that is, a government agent engaged in the enforcement of the criminal laws of the United States, I am authorized to request the issuance of a federal seizure warrant.

I am also an investigating or law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7), in that I am empowered by law to conduct investigations and to make arrests for federal offenses. I furnished the investigative facts contained in the foregoing Verified Complaint for Forfeiture *In Rem*. The investigative facts are based on personal knowledge I obtained from my involvement in the underlying investigation, my review of the relevant investigative material, other federal agencies and law enforcement officers involved in the investigation, other reliable official Government sources, and my own training and experience.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

I hereby verify and declare, under penalty of perjury pursuant to 28 U.S.C. § 1746, that I have read the foregoing Verified Complaint for Forfeiture *In Rem*, that I know its contents, and that the facts it contains are true and correct to the best of my knowledge.

Executed this 8th day of October, 2026.

ANDREW CROPCHO

Digitally signed by ANDREW CROPCHO
Date: 2026.10.08 16:47:00 -07'00'

ANDREW CROPCHO
Special Agent
Federal Bureau of Investigation

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970