KENNETH M. SORENSON
United States Attorney
District of Hawaii

JOSEPH MCGINLEY
Assistant U.S. Attorney
Room 6-100, PJKK Federal Building
300 Ala Moana Boulevard
Honolulu, Hawaii 96850
Telephone: (808) 541-2850
Facsimile: (808) 541-3752
Email: Joseph.McGinley@usdoj.gov

Attorney for Plaintiff
UNITED STATES OF AMERICA

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF HAWAII

UNITED STATES OF AMERICA, Plaintiff, vs. 1,385,380.27152 USDT, Defendant *in Rem*.	Case No. COMPLAINT FOR FORFEITURE; VERIFICATION OF SPECIAL AGENT BRYCE LINDEVIG

COMPLAINT FOR FORFEITURE

Plaintiff United States of America, by its undersigned attorneys, brings this Complaint for Forfeiture and alleges as follows in accordance with Rule G(2) of the Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions, Federal Rules of Civil Procedure:

NATURE OF THE ACTION

1. This is a civil action *in rem* to forfeit and condemn to the use and benefit of the United States the above-captioned property, (1) as property which constitutes or is derived from proceeds traceable to a violation of any offense constituting a specified unlawful activity as defined in 18 U.S.C. § 1956(c)(7), including wire fraud in violation of 18 U.S.C. § 1343, and subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C), and (2) as property that is involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956(a)(1)(B)(i).

2. For its claims against the above-captioned property, the United States alleges as follows upon information and belief.

THE DEFENDANT *IN REM*

3. The above-captioned property includes all right, title, and interest in 1,385,380.27152 USDT[1] (the "Defendant Property"), which was held in two virtual wallet addresses, identified as TBckzYfZmerBiHWVs5cpXqsvzty58xirj8 ("Suspect Address 1") and TEeUUbxFC8jtP3V4fDBVAg6nvfVWeDZt77 ("Suspect Address 2," and with Suspect Address 1, the "(Suspect Addresses"), and seized on May 9, 2025.[2]

[1] Tether, widely known as "USDT", is a blockchain-based cryptocurrency whose tokens in circulation are backed by an equivalent amount of U.S. dollars, making it what is known as a "stablecoin".

[2] Although a seizure warrant for the Defendant Property was served on February 7, 2025, the United States obtained the Defendant Property on May 6, 2025.

4. The Defendant Property is currently being held by the United States Secret Service.

JURISDICTION AND VENUE

5. Plaintiff brings this action *in rem* in its own right to forfeit and condemn the Defendant Property. This Court has subject matter jurisdiction over an action commenced by the United States under 28 U.S.C. § 1345, and over an action for forfeiture under 28 U.S.C. § 1355(a).

6. This Court has *in rem* jurisdiction over the Defendant Property under 28 U.S.C. § 1355(b)(1).

7. Venue is proper in this district pursuant to 28 U.S.C. § 1355(b)(1) and 28 U.S.C. § 1395, because acts or omissions giving rise to the forfeiture occurred in this District, and the action accrued in this district.

BASIS FOR FORFEITURE

8. The Defendant Property is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C), as property, real or personal, which constitutes or is derived from proceeds traceable to a violation of any offense constituting "specified unlawful activity" (as defined in 18 U.S.C. § 1956(c)(7)), or a conspiracy to commit such offense, is subject to forfeiture to the United States. Pursuant to 18 U.S.C. § 1956(c)(7) and 18 U.S.C. § 1961(1), wire fraud in violation of 18 U.S.C. § 1343 is a specified unlawful activity within the meaning of 18 U.S.C. § 981(a)(1)(C).

9. Additionally, the Defendant Property is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A), as property involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956(a)(1)(B)(i), or any property traceable to such property.

CRYPTOCURRENCY TERMS

10. Cryptocurrency (also known as digital currency or virtual currency) are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Cryptocurrency is not issued by a government or bank like traditional fiat currencies such as the U.S. dollar but are generated and controlled through computer software.

11. Tether ("USDT") is a type of cryptocurrency. Payments made with USDT, and other cryptocurrencies, are recorded in a public ledger that is maintained by peer-to-peer verification (i.e., a "blockchain") and is, thus, not maintained by a single administrator or entity.

12. USDT is a blockchain-based cryptocurrency whose tokens in circulation are backed by an equivalent amount of U.S. dollars, making it what is known as a "stablecoin." Individuals can acquire USDT through exchanges (i.e., online companies which allow individuals to purchase, sell or exchange

cryptocurrencies for fiat currencies or other cryptocurrencies), or directly from other addresses which are controlled by an individual/entity.

13. Virtual currency addresses are the particular virtual locations to which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented by a string of alphanumeric characters.

14. Each virtual currency address is controlled through the use of 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.

15. A virtual currency 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 also allows users to send and receive virtual currencies. Multiple addresses can be stored in a wallet.

16. Many virtual currencies publicly record all of their transactions on a "blockchain." The blockchain is essentially a distributed public ledger, run by a decentralized network, containing an immutable and historical record of every transaction utilizing that blockchain's technology. The blockchain can be updated multiple times per hour and record every virtual currency address that ever received that virtual currency. It also maintains records of every transaction and all

the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies.

17. Although the identity of an address owner is generally anonymous (unless the owner opts to make the information publicly available), analysis of the blockchain can often be used to identify the owner of a particular address. The analysis can also, in some instances, reveal additional addresses controlled by the same individual or entity.

18. It is possible to use the blockchain to trace funds forwards and backwards from a single address or a single transaction, not unlike the manner in which investigators can trace the movement of funds in fiat currencies. Despite the anonymized nature of a cryptocurrency blockchain, information identifying the sender, or the recipient of a transaction can be obtained from payment processors or vendors. This information helps investigators identify payment streams, or a single flow of funds over time, belonging to the same pool of funds controlled by the individuals.

BACKGROUND ON "PIG BUTCHERING"

19. "Pig Butchering" or "Sha Zhu Pan" is a type of investment fraud scheme, which oftentimes convinces victims to invest in cryptocurrency through non-existent cryptocurrency trading platforms. The scammer typically initiates contact through social media platforms and eventually form a relationship with the

victim to grow trust. Those relationships may be perceived by the victims as romantic, professional, or friendship based. The scammers often create profiles using fictitious names, locations, images, and personas, allowing the scammers to cultivate personal relationships with prospective victims. The scammers assist the victims with opening a cryptocurrency account, often on a U.S.-based exchange such as Coinbase, Crypto.com or Kraken, and then walk the victim through transferring money from a bank account to that cryptocurrency account. The victims will receive instructions on how to transfer their cryptocurrency assets to the fake investment platform. The scammers promise a lucrative return of investment, by manipulating an increase in balance to the victim's account on their fraudulent domain. The scammers also provide falsified transaction photos that depict that scammers are contributing their own funds to the victim's initial investment.

20. Often enticed by the falsified returns, the victim continues to invest, until they try to retrieve their gains, only to find that they are unable to retrieve them. The scam continues by the scammers demanding additional payments be made to the platform for their investments to be released and/or withdrawn. Examples include, victims being required to pay an additional percentage to the fraudulent platform in order to guarantee the funds, prepay taxes on the balance, or to pay a fee/fine due to suspicious money laundering activities. The "butchering"

or "slaughtering" refers to the victims once their assets are stolen, ultimately causing the victims financial and emotional ruin.

21. The cryptocurrency ecosystem is used by criminals not only to receive victim money, but to launder it quickly, anonymously, and at scale. Like traditional money laundering, laundering money through cryptocurrency shares the same three stages of placement, layering, and integration, with different techniques applied within each:

a. **Placement:** Scammers use non-custodial, or "private" wallets to initially receive victim funds. This is because such wallets are unattributable to law enforcement by blockchain analysis alone, are simple to create, and can accept large transaction amounts without additional scrutiny.

b. **Layering:** Next, scammers will have victim funds traverse numerous private wallets, consolidate with other illegitimate and sometimes legitimate funds, and be subjected to other more cryptocurrency-specific processes to obfuscate both the origin of, and the ultimate destination for, the victim funds.

c. **Integration:** Finally, by using a diffuse network of "brokers," who agree to exchange cryptocurrency for fiat using various

means, criminals render their proceeds liquid and fully integrated with the legitimate financial system.

FACTS GIVING RISE TO FORFEITURE

Summary

22. On or about July 2024, the United States Secret Service Honolulu Field Office learned that a Honolulu, Hawaii-based victim ("Victim-1") reported that she was deceived into sending approximately 180,223 USDT in cryptocurrency to a receiving address. (0x1cbAd99C64AdBD3706741b33A9a49e38898cF3E0) (the "Scam Address") displayed on what turned out to be a scam website: babylonreport.com.[3]

23. Analysts traced cryptocurrency from the Scam Address through multiple transactions, resulting in the identification of the Suspect Addresses, from which the Defendant Property was seized. In the process of tracing the transactions associated with Victim 1's initial investment, analysts were able to identify additional victims of the same or similar investment scams, whose assets flowed through the same virtual addresses.

[3] Several victims associated with the Babylon platform confirmed in interviews that the URL babylonreport.com was taken down during the time the victims were investing; however, the victims were provided alternative but similar URLs including babylonvapes.com, and babylearner.com showing victim's account information.

24. Almost as soon as Victim 1's (and other victims') initial cryptocurrency investment was deposited in the Scam Address, it was stolen immediately by being sent through a series of rapid transfers through various addresses.

The Wire Fraud Scheme

25. On or about March 11, 2024, Victim-1 logged into Facebook to search for investment opportunities to help her earn money, due to having to take an early retirement from the military for medical reasons.

26. After clicking on various advertisements, at some point Victim-1 was added to a Facebook group entitled "Eric investment Team 4."

27. On March 13, 2024, Victim-1 received a Facebook message from an individual with the profile name "Elina Rafael" ("Rafael"), asking Victim-1 to add her as a friend so she could add her to an investment discussion group.

28. Victim-1 ignored the message from Rafael and ignored the communications in "Eric investment Team 4" Facebook group. Victim-1, however, accepted a friend request from an individual with the profile name Eric Lund ("Lund").

29. Lund began discussing cryptocurrency futures trading with Victim-1, and suggested that she speak with his assistant, Rafael.

30. On March 13, 2024, Rafael posted a message in the Facebook group chat introducing herself, stating that the creator of the discussion group was Lund, and that the chat would include discussion about investing in stocks and cryptocurrency. Rafael promised that participants would "continuously multiply [their] assets."

31. Communication in the "Eric investment Team 4" group chat reflected several Facebook user comments that Rafael guided them on how to register or open a "contract account."

32. On or about March 17, 2024, Victim-1 received a message from an individual with a Facebook profile name "Thomas Gonzalez" ("Gonzalez"). "Gonzalez" stated: "Hello! I'm from the same discussion group as you and I found you here, did you just join too?" Over the next several days, "Gonzalez" messaged Victim-1 about daily trading profits and about being able to use a "professional trading APP for any transaction, allowing you to skillfully view all charts and pay attention in a timely manner."

33. It was only once Victim-1 began chatting with "Gonzalez" that she began paying attention to the messages in the "Eric investment Team 4" group chat. The messages reflected multiple Facebook users commenting that they earned large percentage profits.

34. On March 15, 2024, a Facebook user in the "Eric investment Team 4" group chat posted that the people in the group are fake and that it was a scam. That user was removed from the group chat within 3 minutes of her comment.

35. Other supposed Facebook users continued to post in the group chat about making substantial investment gains.

36. On or about March 22, 2024, Victim-1 asked Gonzalez why he was helping her. Gonzalez responded: "I am a very kind person. My parents are very friendly and treat everyone the same. I believe this is our fate."

37. On the same day, Gonzalez asked Victim-1 if she had a crypto wallet. Victim-1 replied that she did not, and asked how to open one. Gonzalez sent Victim-1 a link to a Crypto.com DeFi wallet and told her to download it. Gonzalez also provided Victim-1 a link to the Babylon trading platform: babylonreport.com/regist/recommend/JvXaCj. Gonzalez advised Victim-1 to contact "Rafael" to register for a trading account.

38. Upon Victim-1 chatting with Rafael, Rafael provided Victim-1 a different link than what Gonzalez originally provided to the Babylon trading platform: https://h5.babylonreport.com/#/pages/login/register?inviteCode=Jv9agY.

39. USSS analysts confirmed that upon opening the Babylon trading platform, Victim-1's account showed she had a zero balance. Furthermore, Victim-1's Babylon account still displayed the Scam Address.

40. On multiple dates and similar times, Gonzalez and Rafael communicated with Victim-1 and discussed similar topics regarding investments in Babylon and wrote in a similar style. Upon information and belief, Gonzalez and Rafael are the same person utilizing two different accounts, or are both involved in the fraudulent scheme.

41. On or about March 29, 2025, Victim-1 advised Rafael that she wanted to start with purchasing 500 USDT.[4] Rafael then instructed Victim-1 how to withdraw the USDT, by directing her to click the "External Wallet" tab in Victim-1's Crypto.com DeFi wallet. Rafael then instructed Victim-1 to create a "whitelist," by adding the cryptocurrency address for Victim-1's Babylon account to her Crypto.com DeFi wallet. A "whitelist" is similar to creating a "favorites" list. Adding the Babylon address to her Crypto.com Defi wallet whitelist would allow Victim-1 to withdraw funds from her exchange account.

42. Rafael then instructed Victim-1 to log into her Babylon account, and again provided the Babylonreport.com URL. Victim-1 inquired with "Rafael", "Where I can find the address to copy?", referring to the cryptocurrency address that is linked to Victim-1's Babylon account. "Rafael" directed Victim-1 to find the Babylon account cryptocurrency address in the "Recharge" tab on the platform.

[4] Victim-1 purchased approximately 490 USDT for the 500 USDT due to transaction fees.

"Rafael" provided a screenshot with the QR code identifying the Scam Address. "Rafael" further instructed Victim-1 to select the coin USDT ERC20.

43. Using Rafael's instructions, Victim-1 attempted to confirm the sending of the funds from the Crypto.com DeFi wallet to the Scam Address. However, the transaction failed because the deposited funds had not yet cleared from Victim-1's originating financial institution.

44. On or about March 31, 2024, Gonzalez continued communicating with Victim-1, telling her she was "beautiful" and looked like a "good girl." He then asked Victim-1 if she finalized the two-factor authentication and if needed, she could wire funds directly from her bank, which would make them available in her cryptocurrency wallet. Gonzalez stated: "Do you have a car? If it is convenient to travel, you can go for wire transfer and start trading early to get profits early."

45. On the same day, Rafael instructed Victim-1 to go to her bank and make a wire transfer: "Let's make money together . . . I don't want you miss any profits and I want you to go *[sic.]* to the bank tomorrow and make a wire transfer."

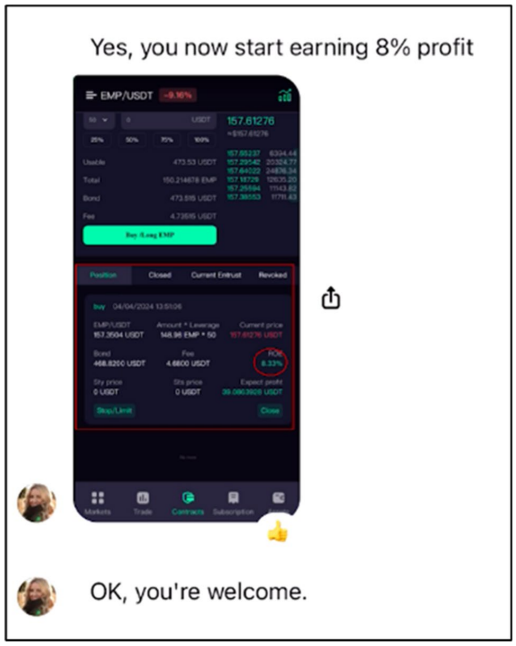
46. Victim-1 subsequently confirmed to Rafael that the funds she requested to be wired to her Crypto.com DeFi wallet were delayed.

47. On April 2, 2024, at approximately 8:26 p.m., Victim-1 advised Rafael that the funds were "finally available."

48. On April 3, 2024, at approximately 6:55 a.m., Rafael instructed Victim-1 to deposit funds into her Babylon account (the Scam Address) and once completed, they would begin trading.

49. On April 4, 2024, Victim-1 advised Rafael that her wire transfer for $2,000 was still being processed, but that $1,000 was available. Rafael instructed Victim-1 to use her entire balance to purchase USDT and transfer the USDT to the Scam Address.

50. Rafael walked Victim-1 through the process and advised her that the transfer was successful. Rafael subsequently showed Victim-1 how to buy cryptocurrency and make trades. Rafael sent an image of the alleged trades, which appeared to look legitimate. Rafael said that Victim-1 would start earning 8% profit:



51. "Rafael" instructed Victim-1 that she had made a 62% profit (based on her initial investment of $947), and that if she invested more than $10,000, she could make $6,200 in profit. "Rafael" proceeded to advise Victim-1 to use more than $20,000 in funds to make "at least 10K profits every day. . . ." The above screenshot reflecting profit was a fictitious earnings statement to strengthen Victim-1's trust in the platform's potential.

52. "Gonzalez" and "Rafael" continued to chat with Victim-1 on different platforms and about investing and other personal matters (love, trust, and friendships).

53. On April 4, 2024, at "Rafael's" suggestion, Victim-1 attempted to transfer $20,000 from her USAA bank account to her Crypto.com DeFi wallet. Victim-1's bank, however, blocked the transfer.

54. On or about April 5, 2024, Victim-1 advised "Rafael" that she had $7,000.00 available in her Crypto.com DeFi wallet. With "Rafael's" assistance, Victim-1 purchased 6,800 USDT, which she moved to the Babylon account controlled by fraudsters (individuals overseeing the operations of the fictitious trading platform – Babylon).

55. Upon further encouragement from "Rafael," on or about April 5, 2024, Victim-1 transferred $70,000 from her traditional investment account to the Crypto.com DeFi wallet to purchase USDT, and then transferred to

the Babylon account controlled by fraudsters (individuals overseeing the operations of the fictitious trading platform – Babylon).

56. Victim-1 was made to believe that the funds were traded and resulted in large profits. Such representations by "Rafael" were false.

57. On or about April 7, 2024, "Rafael" began telling Victim-1 about a "private membership group" with Mr. Eric with very large profits. The conditions for joining such group were "300K funds to join the membership group and get at least 300% profit every day." The following day "Rafael" stated that $250K was required to join. According to "Rafael," membership would bring "huge changes, which will be particularly helpful for your retirement."

58. On or about April 9, 2024, "Rafael" instructed Victim-1 to deposit $40,000 worth of USDT to the Babylon account linked to the Scam Address. Victim-1 was unsuccessful at wiring $35,000, as instructed by "Rafael," so she wired smaller amounts instead. Victim-1 wound up purchasing approximately 34,106 USDT.

59. On or about April 12, 2024, Victim-1's Babylon account appeared to take losses[5]. "Rafael" told Victim-1 to deposit more money to make up for losses.

[5] Victims are lured into fictitious cryptocurrency investment platforms that are entirely controlled by scammers, who manipulate the platform's functionality, including account balances, transaction histories, and withdrawal processes. These platforms falsely display large account balances and significant returns on investment (ROIs) to create the illusion of profitability, while blockchain analysis

Victim-1 responded, "I transferred 10K to start recovering my ridiculous loss." She advised "Rafael" that she would do one more trade, and if she lost more funds, she would cut her losses at that point. Victim-1's Babylon account subsequently showed that she gained over 83%.

60. On or about April 22, 2024, Victim-1 informed "Rafael" that she had deposited $25,000 in her Crypto.com DeFi wallet.

61. On or about April 23, 2024, Victim-1 advised "Rafael" that she had recovered almost $60,000 from her losses from investment trades Victim-1 believed she made, and would continue to wait for instructions from "Rafael."

62. Victim-1's Babylon account (which was linked to the Scam Address and controlled by fraudsters) continued to show losses.

63. On or about May 6, 2024, Victim-1 told "Rafael" that she needed to withdraw funds to show her son the investment was legitimate. "Rafael" told her to avoid large withdrawals, as that might be considered "laundering money." "Rafael" advised Victim-1 to withdraw only a few hundred dollars.

---

reveals that the associated accounts contain zero digital assets. Scammers control the wallet addresses displayed on the platform and block withdrawal attempts by either showing failed transactions or disabling the withdrawal function entirely, ensuring victims cannot access their funds and prolonging the fraud scheme.

64. Victim-1 was never able to withdraw any money, despite multiple attempts. Babylon customer service provided Victim-1 with the following explanations, among others:

a. "[Y]our account is currently not approved by us because you have not completed the real-name authentication."

b. "Your photos are too blurry."

c. "Since your funds exceed 100K, our system needs to strictly verify your identity . . . ."

d. "[Y]our identity verification failed and you need to pay some money."

e. "I just calculated that you need to pay a total of 15385 USDT in taxes."

65. The last message Victim-1 received from "Rafael" was on or about May 8, 2024.

66. Victim-1, however, continued to communicate with "Gonzalez" for help recovering her losses. "Gonzalez" said Victim-1 would need to add more funds to her account. "Gonzalez" advised Victim-1 that she could earn money back if she joined Mr. Eric's "whale program."

67. Victim-1 was never successful in receiving any investment funds.

68. Victim-1 reported the above to law enforcement, along with the supporting documentary materials.

69. In total, as set forth in the table below, Victim-1 sent more than 171,000 USDT total to the Scam Address associated with her Babylon Account:

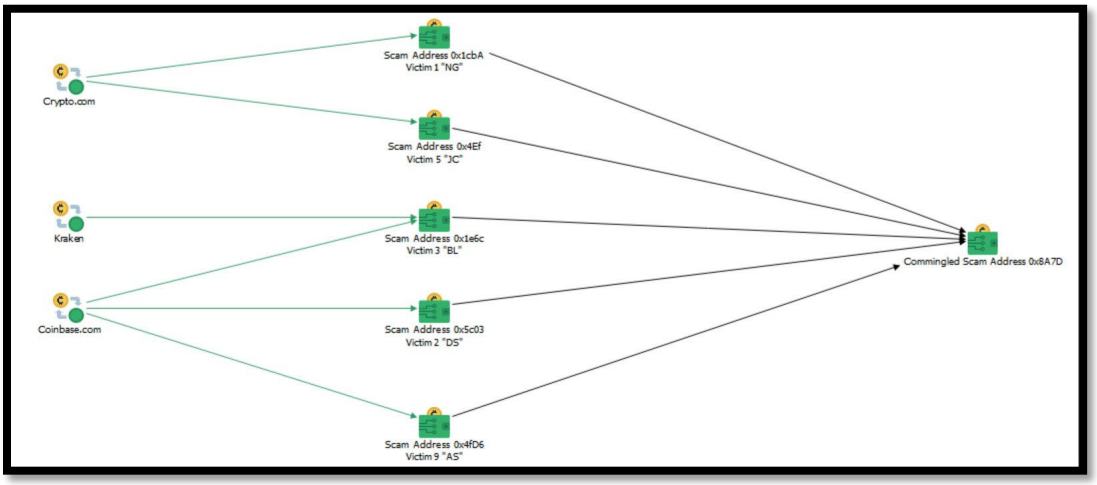
Date	Sending Address	Receiving Address	Amount in USD	Asset
04/04/2024	Crypto.com	Babylon Address 0x1cbAd99C64AdBD3706741b33A9a49e38898cF3E0	947.03	USDT
04/06/2024	Crypto.com	Babylon Address 0x1cbAd99C64AdBD3706741b33A9a49e38898cF3E0	6,619.48	USDT
04/08/2024	Crypto.com	Babylon Address 0x1cbAd99C64AdBD3706741b33A9a49e38898cF3E0	66,238.84	USDT
04/10/2024	Crypto.com	Babylon Address 0x1cbAd99C64AdBD3706741b33A9a49e38898cF3E0	34,090.19	USDT
04/15/2024	Crypto.com	Babylon Address 0x1cbAd99C64AdBD3706741b33A9a49e38898cF3E0	474.68	USDT
04/15/2024	Crypto.com	Babylon Address 0x1cbAd99C64AdBD3706741b33A9a49e38898cF3E0	9,448.94	USDT
04/15/2024	Crypto.com	Babylon Address 0x1cbAd99C64AdBD3706741b33A9a49e38898cF3E0	8,762.17	USDT
04/16/2024	Crypto.com	Babylon Address 0x1cbAd99C64AdBD3706741b33A9a49e38898cF3E0	24,381.12	USDT
04/22/2024	Crypto.com	Babylon Address 0x1cbAd99C64AdBD3706741b33A9a49e38898cF3E0	19,502.27	USDT
04/28/2024	Crypto.com	Babylon Address 0x1cbAd99C64AdBD3706741b33A9a49e38898cF3E0	966.56	USDT

70. A query of Federal Bureau of Investigation's ("FBI's") Internet Crime Complaint Center, resulted in the identification of additional victims who had been defrauded in the same or similar scheme as Victim-1, using the Babylon platform.

Tracing of Fraud Proceeds to the Suspect Addresses

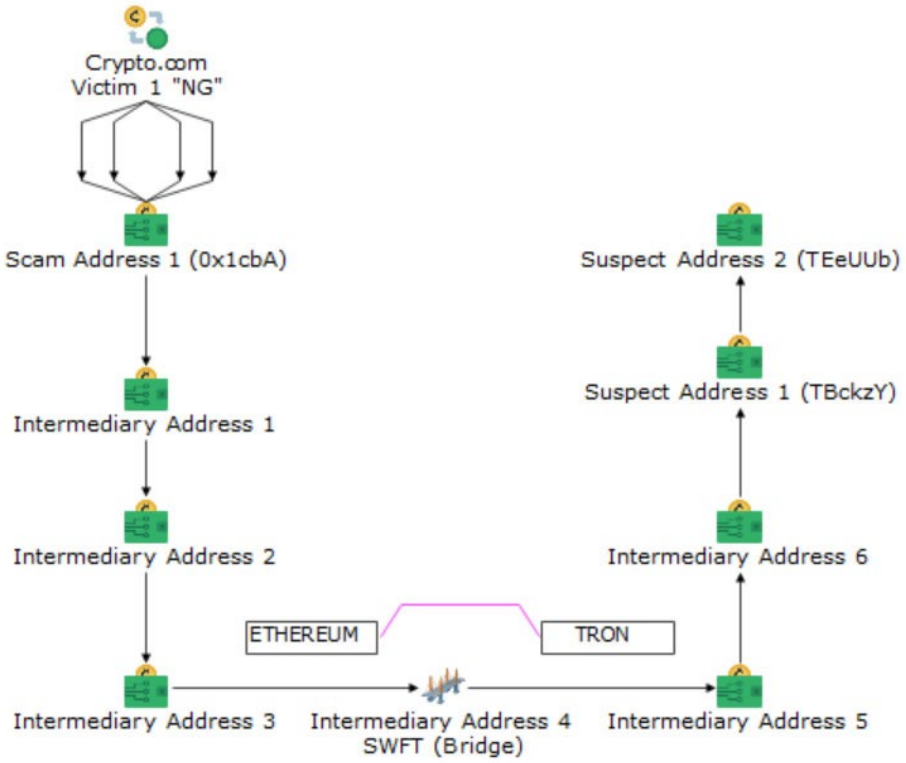
71. The below chart reflects how the funds of Victim-1, and at least four other victims, transferred from their DeFi wallets to different scam addresses associated with their respective Babylon platform account addresses, which were

then ultimately commingled at address 0x8A7De615Cc8902fA965465B7761305284Bc3A80F.



72. **Victim-1.** Victim-1's USDT was transferred through approximately 9 intermediary addresses before being deposited in the Suspect Addresses. All of the intermediary addresses were established between January 2024 and April 2024. All of the accounts exhibited a history of frequent, large dollar deposit transactions, followed by a pattern of rapid movement of funds with large corresponding withdrawals. Despite their short duration of existence, the intermediary addresses processed over $61 million worth of cryptocurrency. The flow of funds through the intermediary addresses also involved transfer between different blockchain networks. All of the above are indicia of attempts to conceal or disguise the nature, location, source, ownership, or control of the wire fraud proceeds and are frequently used in "pig butchering" schemes.

73. The following chart shows the flow of funds from Victim-1's Crypto.com DeFi wallet to the Suspect Addresses.



74. Specifically, the following deposits from Victim-1 were traced to the Suspect Addresses:

a. On or about April 8, 2024, Victim-1 sent 66,238.84 USDT to the Scam Address from her Crypto.com DeFi wallet. On April 10, 2024, Victim-1 sent approximately 34,090.19 USDT to the Scam Address from her Crypto.com DeFi wallet. Prior to such transactions, the Scam Address held a zero balance.

b. On April 12, 2024, the Scam Address sent the 100,329 USDT (deposits from Victim-1) to an intermediary address 0x8A7De615Cc8902fA965465B7761305284Bc3A80F ("0x8A7D").

c. Prior to receiving the above deposit constituting proceeds of the fraud on Victim-1, 0x8A7D had a balance of approximately 149,425 USDT (over 14,000 USDT of which was traceable to another victim of the same or similar fraud using the Babylon platform). Shortly after receiving the deposit, 0x8A7D received an additional 144,142 USDT in five deposits from unknown addresses.

d. Still on April 12, 2024, minutes later, 0x8A7D commingled the funds it received, and sent approximately 390,000 USDT to another intermediary address 0x7Cd5d7783aB66fA7538Ac6a6992cBD85d6ad2AD3 ("0x7Cd5").

e. Prior to receiving the 390,000 USDT, 0x7Cd5 held approximately .50 USDT. The next transaction conducted by 0x7Cd5 occurred on April 15, 2024, when 390,000 USDT was transferred from 0x7Cd5 to a third intermediary address 0xbb12810ceD7B0f4a42D65280248e0CFde63BAa78 ("0xbb12), thereby leaving 0x7Cd5 with approximately .50 USDT.

f. Prior to receiving the 390,000 USDT transfer from 0x7Cd5, 0xbb12 had a zero balance. Shortly after receiving the 390,000 USDT, 0xbb12 transferred the funds into a SWFT Bridge protocol, via transaction hash 0x80479f2b41cd595c15cb6ef17f1bb6eabfe62c25ac5e52d861f31cf3c6822799,

which bridged the 390,000 USDT from the Ethereum network to the Tron network. After feeds were paid, the transaction resulted in 388,828 USDT-Tron being received by another intermediary address TKW2Syjm7dw6K6MuNiPDLGaRjh2tT2JP4V ("TKW2Sy").

g. Prior to the transfer of the 388,828 USDT-Tron, TKW2Sy held a balance of 0.01 USDT-Tron. Minutes later, TKW2Sy sent the 388,828 USDT-Tron to yet another intermediary address TKB7efpF9mimRwRzwQZpKoDCqmAVjbvxA4 ("TKB7ef").

h. Prior to the transfer of the 388,828 USDT-Tron, TKB7ef held a balance of approximately 0.30 USDT-Tron. After receiving the transfer, TKB7ef received approximately 103,399 USDT-Tron from TKW2Sy, funds which also constitute proceeds of the fraud on Victim-1. The funds were commingled and 279,900 USDT-Tron from TKB7ef was transferred to Suspect Address 1 on April 15, 2024.

i. Prior to the deposit of the 279,900 USDT-Tron, Suspect Address 1 held a balance of approximately 205,286 USDT-Tron. After receiving the transfer, on April 15, 2024, Suspect Address 1 sent 195,000 USDT-Tron to Suspect Address 2, leaving Suspect Address 1 with a balance of approximately 185,186 USDT-Tron.

j. Prior to receiving the transfer of the 195,000 USDT-Tron, Suspect Address 2 had a balance of approximately 1,318,897 USDT-Tron. Suspect Address 2 continued to send and receive funds; however, the balance never reached a zero USDT-Tron amount.

k. At the time the seizure warrant was executed as to the Suspect Addresses, Suspect Address 2 continued to hold approximately 110,253 USDT-Tron of the proceeds of the fraud on Victim-1 and approximately 14,360 USDT-Tron belonging to another victim's funds that were specifically traced.

75. In addition to the tracing set forth above, the following additional deposits from Victim-1 were traced to Suspect Address 1:

Table 3: Victim 1 "NG" funds traced to Suspect Address 1

Date	Amount	Asset
04/05/2024	947.03	USDT
04/06/2024	6,619.48	USDT
04/15/2024	8,762.17	USDT
04/16/2024	24,381.12	USDT
04/22/2024	19,502.27	USDT
04/28/2024	966.56	USDT

76. Law enforcement was also able to trace 9,796 USDT of proceeds of the Babylon investment fraud on Victim-2 to Suspect Address 1.

77. The lowest balance Suspect Address 1 reached was 53,140.20 USDT-Tron. Accordingly, using the Lowest Intermediate Balance Rule account, most of

the funds seized from Suspect Address 1 are proceeds of wire fraud. Additionally, all such funds are involved in concealment money laundering.

78. On or about August 14, 2024, Tether voluntarily froze the USDT in the Suspect Addresses.

79. Tether subsequently, on August 19, 2024, received an inquiry from "Zhang Zhang" using email address xl2tlwra@icloud.com, claiming to be the owner of Suspect Address 1. A day later, Tether received an inquiry from a different email address, claiming ownership of the funds in Suspect Address 1: alyciadev6@gmail.com.

80. On August 20, 2024, Tether received an inquiry from litaholliuhpkc7555@gmail.com, claiming ownership of Suspect Address 2.

81. On September 19, 2024, Tether received an inquiry from lativshivkova@gmail.com, claiming ownership of Suspect Address 2. On the same day, Tether received an inquiry from elianayfabrico10@gmail.com, claiming ownership of Suspect Address 1. Both claimants provided the same identification documents.

82. On December 26, 2024, Tether received claims of ownership to Suspect Address 1 and 2 from two different email addresses: SarahGordon1968520@outlook.com and KathrynHopkins20010@outlook.com.

83. Only two of the parties contacted USSS to pursue their ownership claim, but neither responded to a request for additional proof of ownership and source of the funds for each address.

84. On or about February 5, 2025, Magistrate Judge Wes Reber Porter approved a seizure warrant, authorizing the seizure of all funds in the Suspect Addresses, on the grounds that there was probable cause to believe that the entire contents of the Suspect Addresses were proceeds of wire fraud, or traceable thereto and/or involved in concealment money laundering. The execution of the seizure warrant on May 9, 2025 resulted in the seizure of **1,385,380.27152 USDT ($1,385,380.27 USD) –** the Defendant Property.

FIRST CLAIM FOR RELIEF
(18 U.S.C. § 981(a)(1)(C))

85. The United States incorporates by reference the allegations set forth in Paragraphs 1 through 84 above, as if fully set forth herein.

86. The Defendant Property is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C) as property which constitutes or is derived from proceeds traceable to a violation of any offense constituting "specified unlawful activity" or a conspiracy to commit such offense. Specifically, the Defendant Property constitutes proceeds of wire fraud in violation of 18 U.S.C. § 1343—the proceeds of the "pig butchering" scheme committed against Victim-1 and the other victims.

SECOND CLAIM FOR RELIEF
(18 U.S.C. § 981(a)(1)(A))

87. The United States incorporates by reference the allegations set forth in Paragraphs 1 through 84 above, as if fully set forth herein.

88. The Defendant Property is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A) as property that is involved in a violation of 18 U.S.C. 1956(a)(1)(B)(i), or property traceable to such property.

WHEREFORE, the United States prays that:

1. Notice of this action be given to all persons who reasonably appear to be potential claimants of interests in the Defendant Property;

2. The Defendant Property shall be forfeited and condemned to the United States of America;

3. Plaintiff be awarded its costs and disbursements in this action; and

//

//

//

//

//

//

//

4. The Court award such other and further relief as this Court deems just and proper.

DATED: March 9, 2026, at Honolulu, Hawaii.

KENNETH M. SORENSON
United States Attorney
District of Hawaii

/s/ *Joseph McGinley*
By _____
JOSEPH MCGINLEY
Assistant U.S. Attorney

Attorneys for Plaintiff
UNITED STATES OF AMERICA

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF HAWAII

UNITED STATES OF AMERICA, Plaintiff, vs. 1,385,380.27152 USDT, Defendant *in Rem*.	Civil No. VERIFICATION OF BRYCE LINDEVIG

VERIFICATION OF BRYCE LINDEVIG

I, Bryce Lindevig, declare that:

I am a Special Agent of the United States Secret Service. I have read the attached Complaint for Forfeiture and know the contents thereof; the information contained in the Complaint for Forfeiture has been furnished by official government sources; and, based on information and belief, the allegations contained in the Complaint for Forfeiture are true.

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

Executed on January 7, 2026, at Honolulu, Hawaii.

BRYCE LINDEVIG