

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

vs.

No. 1:26-cv-1575

729,279.70 USDT associated with virtual currency address ending qqDTH (Subject Address 1) associated with email addresses ffss700666@gmail.com, boxingwash999888@gmail.com, and dqzh1234567@163.com (25-FBI-006097),

3,647.65 USDT associated with virtual currency address ending 52YM5 (Subject Address 2) associated with email address paulwash999888@gmail.com (25-FBI-006096),

125,733.5482 USDT associated with virtual currency address ending eWa4B (Subject Address 3) associated with email address boxingwash999888@gmail.com and tdcx700728@163.com (25-FBI-006098),

and

7,047,805.56574407 Cardano (ADA) associated with User ID ending 9131 with email address ass1090427@icloud.com at Binance, Abu Dhabi, UAE (26-FBI-002202),

Defendant Property.

VERIFIED COMPLAINT FOR FORFEITURE IN REM

NOW COMES Plaintiff, United States of America, by and through its attorneys, Timothy P. Verhey, United States Attorney for the Western District of Michigan, and Daniel T. McGraw, Assistant United States Attorney, and states upon information and belief that:

NATURE OF ACTION

1. This is a civil forfeiture action filed pursuant to 18 U.S.C. §§ 981(a)(1)(A), 981(a)(1)(C), 982(a)(1) and Supplemental Rule G(2) of the Federal Rules of Civil Procedure to forfeit and condemn to the use and benefit of the United States of America the following property:

- a. 729,279.70 USDT associated with virtual currency address ending qqDTH (Subject Address 1) associated with email addresses ffss700666@gmail.com, boxingwash999888@gmail.com, and dqzh1234567@163.com (25-FBI-006097),
- b. 3,647.65 USDT associated with virtual currency address ending 52YM5 (Subject Address 2) associated with email address paulwash999888@gmail.com (25-FBI-006096),
- c. 125,733.5482 USDT associated with virtual currency address ending eWa4B (Subject Address 3) associated with email address boxingwash999888@gmail.com and tdcx700728@163.com (25-FBI-006098), and
- d. 7,047,805.56574407 Cardano (ADA) associated with User ID ending 9131 with email address ass1090427@icloud.com at Binance, Abu Dhabi, UAE (26-FBI-002202)

(the “Defendant Property”).

THE DEFENDANT IN REM

2. The Defendant Property consists of virtual currency, also known as cryptocurrency, that was seized on or about December 17, 2025 (from Subject Addresses 1, 2, 3) and on or about April 29, 2026 (from User ID ending 9131) by the Federal Bureau of Investigation (“FBI”) pursuant to seizure warrants authorized by the United States District Court for the Western District of Michigan. The Defendant Property is currently in the custody of the United States Marshals Service (“USMS”).

JURISDICTION AND VENUE

3. This Court has jurisdiction over this proceeding pursuant to 28 U.S.C. §§ 1345 and 1355(b)(1)(A), because this action is being commenced by the United States of America as Plaintiff, and the acts giving rise to the basis for forfeiture occurred in this judicial district.

4. Venue is proper before this Court pursuant to 28 U.S.C. § 1355(b)(1) because the acts or omissions giving rise to forfeiture occurred in this judicial district, and/or pursuant to 28 U.S.C. § 1395(b), because the Defendant Property was found within this judicial district.

BASIS FOR FORFEITURE

5. As set forth below, the Defendant Property is subject to civil forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(A) because it is any property, real or personal, involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956(a)(1)(B)(i) (concealment money laundering), and in violation of 18 U.S.C. § 1956(h) (money laundering conspiracy), or any property traceable to such

property; and pursuant to 18 U.S.C. § 981(a)(1)(C), because it is any property, real or personal, which constitutes or is derived from proceeds traceable to wire fraud, in violation of 18 U.S.C. § 1343.

6. Under 18 U.S.C. § 1956(a)(1)(B)(i), it is a criminal offense for anyone, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conducts such a financial transaction which in fact involves the proceeds of specified unlawful activity, knowing that the transaction is designed in whole or in part, to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of the specified unlawful activity, here, wire fraud, in violation of 18 U.S.C. § 1343.

7. Under 18 U.S.C. § 1956(h), it is a criminal offense to conspire to commit any offense described in section 1956, including 1956(a)(1)(B)(i).

8. Under 18 U.S.C. § 1343, it is a criminal offense for anyone who has devised a scheme or artifice to defraud, or anyone who has devised a scheme or artifice to obtain money by means of false or fraudulent pretenses, representations, or promises, to transmit by means of wire, radio, or television communication in interstate commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing the scheme or artifice.

FACTS SUPPORTING FORFEITURE

Background on Virtual Currency (also known as Cryptocurrency)

9. Virtual currencies are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Virtual currencies are not issued

by any government or bank, like traditional fiat currencies such as the U.S. dollar, but are generated and controlled through computer software. Bitcoin (“BTC”) is the most well-known virtual currency in use.

10. 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 string of alphanumeric characters. Each virtual currency address is controlled through a unique corresponding private key—the 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.

11. Many virtual currencies publicly record their transactions on what is referred to and known as the “blockchain.” The blockchain is essentially a distributed public ledger, run by a decentralized network, containing an immutable record of every transaction that has ever occurred using that blockchain’s specific technology. The blockchain can be updated multiple times per hour and records 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.

12. 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 user. A user of virtual currency can operate multiple addresses at any given time and there is no limit to the number of addresses any user can have.

13. 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 single wallet.

Background on Stablecoins

14. Stablecoins are a type of virtual currency whose value is pegged to a commodity's prices, 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.

15. Tether Limited is a company that manages the smart contracts and the treasury (*i.e.*, the funds held in reserve) for USDT. The value of USDT is tied to the value of the U.S. dollar. According to Tether Limited, one USDT is backed by one U.S. dollar held in Tether Limited's reserves. For this reason, USDT is known as a "stablecoin"—a term used to describe a virtual currency that has a value pegged to a fiat currency or the value of a commodity. USDT is hosted on the Ethereum (ETH) and Tron blockchains, among others.

Background on Virtual Currency Exchanges (including Binance)

16. A virtual currency exchange is an online marketplace or platform that allows users to buy, sell, and trade various virtual currency, such as Bitcoin or USDT, using fiat currencies, like USD, or other virtual currencies. Virtual currency exchanges can be centralized (including Binance, Coinbase, Kraken, and Gemini), meaning it operates as a trusted middleman similar to traditional stock exchanges, or decentralized, meaning the platform uses smart contracts to facilitate trading directly between users without a central intermediary (including Uniswap, Pancake Swap, and dYdX). Binance is the largest virtual currency exchange in terms of daily trading volume of virtual currencies.

Chinese Authority Impersonation Scheme

17. FBI is investigating a Chinese Authority Impersonation scheme that targets United States-based Chinese-speaking individuals, causes them to think they are under investigation by Chinese authorities, and fraudulently induces the victims to transfer money to avoid further sanction or consequence.

Victim S.C.

18. During an interview with the FBI, victim S.C. said they currently live in Grand Rapids, Michigan and were born in China. S.C. is a native Mandarin speaker, and has lived in the United States for the past 30 years.

19. On or about June 2, 2025, S.C. received a phone call from an individual purporting to be from Sam's Club. The person spoke to S.C. in Mandarin and advised that they worked in a Sam's Club department that handled issues with Chinese

customers. The person said they identified a credit card that was opened in S.C.'s name and asked for information about specific transactions and purchases that were sent to S.C.'s home and rental property. The person told S.C. they needed a police report number related to the incident and that they would initiate a call into the Hangzhou¹ police department.

20. S.C. was then put in contact with a purported representative from the Hangzhou police department ("Yang"). Yang told S.C. that they were a suspect in a criminal investigation into human/child trafficking and money laundering being conducted in China. Yang said that because S.C. did not appropriately protect their identity, they could be arrested for their role in the case. Yang shouted at S.C. and due to the pressure exerted, S.C. sent, via iMessage, their passport and driver's license pictures. Yang communicated with S.C. from the Apple account zhejiang.cn.110@icloud.com. S.C. was then put in contact with the purported lieutenant on the case ("Hu").

21. Hu told S.C. that their identity was associated with a bank account that had over \$5,000,000 in illicit proceeds. Hu, like Yang, told S.C. they did not appropriately protect their identity from being used and thus was being investigated. For Hu to monitor S.C., S.C. was required to "check in" with Hu, i.e., send their location and what they were doing, every three hours. S.C. was not allowed to tell friends or family what was happening, otherwise they too would become suspects in the case. Hu communicated with S.C. from the Apple account

¹ Hangzhou is the capital city of the Chinese province Zhejiang.

project575868cn@icloud.com. S.C. was harassed for the next couple of weeks by Hu and Yang, and was constantly threatened with arrest and extradition to China. S.C. was sent pictures of their house and of them at a local park to show they were being watched.

22. S.C. was told that, due to the purported criminal case involving money laundering, Hu and Yang needed to do a full review of their finances. S.C. shared details with Hu and Yang about their retirement savings and other assets. S.C. was pressured by Hu to withdraw their retirement account. When S.C. refused, Hu put S.C. in contact with the purported prosecutor on the case (“Tong”).

23. Tong told S.C. that for them to not face extradition to China, S.C. needed to transfer their money to a bank account the “Chinese Police” controlled for review. Tong communicated with S.C. from the Apple accounts tongbeijing110@icloud.com and beijing.tong.110@icloud.com. S.C. eventually complied and withdrew part of their retirement savings and sent \$738,000 to a PNC bank account to an individual in New Jersey with the initials S.L.

Victim M.W.

24. FBI also interviewed M.W., who was born in China, is a native Mandarin speaker, and has lived in the United States for the past ten years.

25. On or about March 28, 2025, M.W. received six straight phone calls from the same number until they finally answered. The caller identified themselves in Mandarin as “Jason Wong” (“Wong”), a purported representative from Costco. Specifically, Wong told M.W. he was calling about transactions made at a Costco that

M.W. regularly frequented that were deemed fraudulent. M.W. pushed back but Wong told M.W. that a Costco credit card was opened in M.W.'s name and listed a Chinese address as the mailing address. Wong told M.W. that M.W. needed to report the incident to the police in Ningbo;² a city that M.W. was familiar with based on where they grew up in China.

26. M.W. was then put in contact with a purported representative from the Ningbo police department. Like what happened to S.C., M.W. was put in contact with Yang, who again used the Apple account zhejiang.cn.110@icloud.com, and was told they were a suspect in a transnational human trafficking case. Yang shouted at M.W., told them M.W.'s name was on a bank account that received approximately \$5,000,000 in illicit proceeds, and that there was an outstanding warrant for their arrest.

27. M.W. was required to "check in" with Yang, i.e., send M.W.'s location and what M.W. was doing every three hours. M.W. was not allowed to tell any friends or family what was happening. M.W. was then put in contact with the purported prosecutor on the case, whose name was Tong, the same name used with S.C.

28. Tong sent a picture of M.W. and M.W.'s partner to show that they were watching. Tong then convinced M.W. that M.W. needed to transfer all M.W.'s money to the purported Chinese police so that they could determine if the money was "clean" or "dirty." Tong again used the Apple accounts beijing.tong.110@icloud.com and tongbeijing110@icloud.com to communicate with M.W. Over the next couple of

² Ningbo is a city in the Chinese province Zhejiang.

months, M.W. transferred nearly all of their household savings, approximately \$350,000, at the direction of Tong. M.W. was also coerced into borrowing approximately \$200,000, which M.W. then transferred at the direction of Tong.

29. Specifically, M.W., between April and June 2025, M.W. transferred approximately \$355,000 to bank accounts associated with S.L., the same recipient who received S.C.'s \$738,000 transfer.

Victim K.L.

30. FBI also interviewed K.L., who was born in China and is a native Mandarin speaker.

31. On or about April 25, 2025, K.L. received a phone call from a purported representative from Costco. The purported representative spoke Mandarin, referenced a property owned by K.L., and inquired about an online purchase that had not been picked up. K.L. advised they had not ordered the product to which the purported representative told them there was also a credit card opened in their name in Hangzhou, China. K.L. was eventually told they needed to file a report with the Hangzhou police, and the call was transferred to the "police."

32. During the call with the purported Hangzhou police, K.L. was told their name was on a bank account that laundered more than \$508,000. Further, K.L. was alleged to have taken 10% of these funds for themselves. K.L. was then required to "check in," i.e., send K.L.'s location and what K.L. was doing every three hours. The purported police officer contacted K.L. from the account project575868cn@icloud.com. I recognized this as the same account used by the purported police that spoke to S.C.

33. In late June 2025, K.L. was contacted by an “inspector” on the case using the account beijing.tong.110@icloud.com. K.L. was told they were responsible for the funds they allegedly took from the laundered bank account. Thus, K.L. transferred approximately \$285,000 to a bank account controlled by the “Chinese Police” to prove its legitimacy.

34. According to records reviewed by FBI, the bank account that received \$285,000 from K.L. was also associated with S.L, the same individual who received transfers from S.C. and M.W.

Victim X.Z.

35. FBI also interviewed the daughter of X.Z., who was born in China, is a native Mandarin speaker, and lived in the United States for approximately 30 years.

36. In or about May 2025, X.Z. received a phone call from an individual purporting to be from Sam’s Club about an order unknown to X.Z. Like S.C., M.W., and K.L., X.Z. was transferred to a purported Chinese police officer who told X.Z. that X.Z. was a suspect in an international money laundering case.

37. The purported police officer threatened X.Z. with arrest and extradition and required X.Z. to “check in,” i.e., send their location and activities every three hours. X.Z. was sent pictures of X.Z.’s spouse in public to show that they were watching X.Z.’s family.

38. X.Z. was required to transfer funds to the Chinese police officers as part of the purported case. Again, the perpetrators communicated with X.Z. via Apple accounts project575868cn@icloud.com, tongbeijing110@icloud.com, and

beijing.tong.110@icloud.com. X.Z. transferred more than \$2,000,000 to the “Chinese Police” as part of the fraud. Specifically, X.Z. transferred \$1,950,000 to an account associated with a person in Illinois, Y.Y.

Victim S.L.

39. FBI interviewed S.L., who is a Chinese national living in New Jersey while attending a university. On or about March 23, 2025, S.L. was contacted by a Mandarin speaking person who purported to be from Costco about alleged transactions conducted in their name. S.L. was eventually referred to a Chinese police department where they learned they were part of an international child abduction case. Specifically, S.L. was told their name was on a bank card that conducted transactions on behalf of the criminal case. S.L. was then required to “check in,” i.e., send their location and activities to the purported Chinese police. The “Chinese police officer” communicated with S.L. using the Apple account project575868cn@icloud.com.

40. S.L. was eventually referred to a purported Chinese prosecutor with the same name that other victims encountered, Tong. Tong communicated with S.L. from the Apple accounts tongbeijing110@icloud.com and tong.beijing110@icloud.com. At Tong’s direction, S.L. opened multiple bank accounts and virtual currency accounts to assist with moving money on behalf of the “Chinese police.” During this time, S.L. was threatened with arrest, required to endure multiple “interrogations,” and was not allowed to tell friends and family what was going on.

41. S.L. began to receive large amounts of money into their newly opened bank accounts from unknown third parties. I now know that these unknown third parties were victims or others associated with the Chinese Authority Impersonation scheme. S.L. transferred these monies to their virtual currency exchange accounts at Kraken and Coinbase.

42. S.L. was also instructed to create a MetaMask³ wallet. S.L.'s MetaMask Ether⁴ address ended in "49dff3." S.L. told me they were instructed to withdraw virtual currency from their Kraken and Coinbase accounts as Eth to their address ending in ("49dff3"). From there, S.L. was told to transfer all of the Eth to a "regulatory" address controlled by the Chinese police that ended in "99C6FE." S.L. told me that all the money transacted through their Coinbase, Kraken, and MetaMask address was "dirty money" that they moved solely at the direction of and as part of the fraud scheme.

43. According to records from Kraken and Coinbase, between April and June 2025, S.L. transferred approximately 442 Ether to their MetaMask address ("49dff3"). As of August 19, 2025, 442 Ether was valued at approximately \$1,833,878.⁵

³ According to their advertisement on the Apple Store, MetaMask is a crypto wallet that can be downloaded to a mobile phone. It has over 100 million user and allows users to buy, sell, and virtual currency.

⁴ Ether is the native cryptocurrency token on the Ethereum blockchain. Ether is typically denoted as "Eth."

⁵ Although this was the value of the Ether as of August 19, 2025, this value differs from the approximate valuations done at the time of the transactions.

44. According to a review of the Ethereum blockchain, more than 99.99% of all Ether that was deposited into S.L.'s MetaMask address ("49dff3") was withdrawn to the "regulatory address" ("99C6FE"), which is another virtual currency address associated with the Chinese Authority Impersonation fraud scheme.

45. According to the public blockchain, "99C6FE" only had incoming deposits and outgoing withdrawals between January 31, 2025 and July 19, 2025. More than 99.99% of all the Ether received was withdrawn to a virtual currency address ending in "E72815."

46. According to the public blockchain for information associated "E72815," all Ether was transferred from the Ethereum blockchain to the Arbitrum⁶ blockchain utilizing a decentralized virtual currency exchange called rubic.exchange.⁷ Upon information and belief, decentralized exchanges are virtual currency trading platforms or marketplaces that operate directly between virtual currency traders, without an intermediary or centralized exchange. Utilizing decentralized exchanges to convert from one type of virtual currency to another, or to move one currency to a different blockchain, is a common technique used to obfuscate or disguise the origination and destination of virtual currency assets.

47. According to tracing of the Ether received by "E72815" on the Arbitrum blockchain, nearly all of it was deposited into two accounts at the virtual currency

⁶ According to their public website, the Arbitrum blockchain is a "layer 2 scaling solution designed to enhance your Ethereum experience."

⁷ According to their public website, Rubic exchange is a "decentralized instant crypto exchange that aggregates 220+ DEXs and cross-chain bridges."

exchange OKX, two accounts at the virtual currency exchange Binance, and two accounts at the virtual currency exchange Bybit.

48. According to records from OKX, Binance, and Bybit, an account holder with the subscriber email address “boxingwash999888@gmail.com” had one of the accounts at OKX, Binance, and Bybit, and an account holder with the subscriber email address “paulwash999888@gmail.com” had the other account at OKX, Binance, and Bybit. Each email address contained “wash999888” in the gmail address.⁸

49. According to records from Binance and Bybit, each account at Binance’s first deposit occurred on March 27, 2025, and each account at Bybit’s first deposit occurred on April 30, 2025.

50. Both account holders provided Taiwan identification documents to all three exchanges (OKX, Binance, and Bybit). Upon information and belief, the primary language spoken in Taiwan is Mandarin; the same language used to facilitate the Chinese Authority Impersonation fraud scheme.

Subject Address 1

51. According to records for “boxingwash999888@gmail.com’s” OKX, Binance, and Bybit accounts, the deposits of Ether were withdrawn as USDT on the Tron blockchain. In total, between April 25, 2025 and August 7, 2025, the three accounts withdrew approximately 5,515,924.71 USDT to virtual currency address

⁸ Upon information and belief, terms like “wash” and “clean,” in the context of money laundering investigations, are used to describe the process of making “dirty money,” or illicit fraud proceeds, appear legitimate, by obfuscating or disguising the origination and ultimate destination.”

ending qqDTH (Subject Address 1). According to records and information received from Tether Compliance, as of August 19, 2025, 729,279.500005 USDT remained in Subject Address 1. The IP Address of the user of Subject Address 1 was located in Taiwan.

52. On or about December 17, 2025, pursuant to a seizure warrant authorized by the United States District Court for the Western District of Michigan, FBI seized 729,279.70 USDT associated with virtual currency address ending qqDTH (Subject Address 1). Between on or about August 19, 2025 and on or about March 31, 2026, email addresses ffss700666@gmail.com, boxingwash999888@gmail.com, and dqzh1234567@163.com contacted the FBI and Tether Compliance and claimed ownership over Subject Address 1 (25-FBI-006097), which is a portion of the Defendant Property and in the custody of USMS.

Subject Address 2

53. According to records for “paulwash999888@gmail.com’s” OKX, Binance, and Bybit accounts, the deposits of Ether were withdrawn as USDT on the Tron blockchain. In total, between April 25, 2025 and August 7, 2025, the three accounts withdrew approximately 4,438,348.66 USDT to virtual currency address ending 52YM5 (Subject Address 2). According to records and information received from Tether Compliance, as of August 19, 2025, 3,645.439013 USDT remained in Subject Address 2. The IP Address of the user of Subject Address 2 was located in Taiwan.

54. On or about December 17, 2025, pursuant to a seizure warrant authorized by the United States District Court for the Western District of Michigan, FBI seized 3,647.65 USDT associated with virtual currency address ending 52YM5

(Subject Address 2) associated with email address paulwash999888@gmail.com (25-FBI-006096), which is a portion of the Defendant Property and in the custody of USMS.

Subject Address 3

55. According to records and information received from Tether Compliance, on or about August 20, 2025, “boxingwash999888@gmail.com” contacted Tether Compliance to claim ownership over Subject Address 3. According to the transactional history associated with Subject Address 3, it received approximately 2,870,071 USDT from Subject Address 1 and Subject Address 2. According to records and information received from Tether Compliance, as of August 19, 2025, 125,733.548202 USDT remained in Subject Address 3.

56. On or about December 17, 2025, pursuant to a seizure warrant authorized by the United States District Court for the Western District of Michigan, FBI seized 125,733.5482 USDT associated with virtual currency address ending eWa4B (Subject Address 3) associated with email addresses boxingwash999888@gmail.com and tdcx700728@163.com (25-FBI-006098), which is a portion of the Defendant Property and in the custody of USMS.

Tracing \$1,950,000 in fraud proceeds transferred from X.Z.

57. According to records of the virtual currency accounts of Y.Y., the recipient of approximately \$1,950,000 in fraudulently transferred funds from X.Z., in July 2026, Y.Y. transferred approximately 577 Ether from their virtual currency

accounts to a virtual currency address ending “5bd294.” As of August 18, 2025, 577 Ether was valued at approximately \$2,393,999.⁹

58. Like the transfers from the virtual currency accounts of S.L., described above, nearly all the 577 Ether transferred out of Y.Y.’s accounts from the Ethereum blockchain to the Arbitrum blockchain. Nearly all were deposited into the same two accounts at OKX, Binance, and Bybit, again associated with boxingwash999888@gmail.com and paulwash999888@gmail.com. According to the withdrawal activity from boxingwash999888@gmail.com’s OKX, Binance, and Bybit account, again, the deposits of Ether were withdrawn as USDT on the Tron blockchain. In total, between April and August, 2025, the three accounts withdrew approximately 5,515,924.71 USDT to a virtual currency address ending “qqDTH” (Subject Address 1).

59. According to the public Tron blockchain, between June and July, 2025, approximately 2,009,016 USDT were transferred to a virtual currency address ending “AJmpX.” Further, in June 2025, “AJmpX” sent approximately 2,001,027 USDT to Binance User ID ending 9131. In addition, between July and August, 2025, “qqDTH” (Subject Address 1) transferred approximately 1,636,196 USDT to a virtual currency address ending “eWa4B.” In August 2025, “eWa4B” transferred approximately 225,813 USDT to a virtual currency address ending “38E37.” According to the

⁹ Although this was the value as of August 19, 2025, this value differs from the approximate valuations done at the time of the transactions.

withdrawal activity for “38E37,” between April 2024 and January 2025, “38E37” transferred approximately 7,842,279 USDT to Binance User ID ending 9131.

60. According to the withdrawal activity from paulwash999888@gmail.com’s OKW, Binance, and Bybit accounts, again, the deposits of Either were withdrawn as USDT on the Tron blockchain. In total, between April and August, 2025, the three accounts withdrew approximately 4,438,348.66 USDT to a virtual currency address ending “52YM5.” According to the Tron blockchain, between May and July, 2025, approximately 2,254,438 USDT were transferred to the virtual currency address ending “AJmpX,” which is the same address that received approximately 2,009,016 USDT from “qqDTH” (Subject Address 1) and sent approximately 2,001,027 USDT to Binance User ID ending 9131.

61. According to records from Binance for Binance User ID ending 9131, this user is associated with an individual from Taiwan and e-mail address “ass1090427@icloud.com,” and it was opened in 2022. However, approximately 90% of the deposits into this account occurred between April 2024 and June 2025.

62. According to records received from Apple, the e-mail accounts used to facilitate this fraud scheme, i.e., tongbeijing110@icloud.com, beijing.tong.110@icloud.com, project575868cn@icloud.com, and zhejiang.cn.110@icloud.com, were accessed from the same IP Addresses used to access Binance User ID ending 9131. Specifically:

- a. IP address 49.213.18.23
 - i. Binance User ID ending 9131 accessed on November 25, 2024

- ii. beijing.tong.110@icloud.com accessed on November 25, 2024
 - iii. Binance User ID ending 9131 accessed on November 27, 2024
 - iv. zhejiang.cn.110@icloud.com accessed on November 28, 2024
- b. IP address 49.213.18.28
- i. Beijing.tong.110@icloud accessed on January 14, 2025
 - ii. Binance User ID ending 9131 accessed on January 16, 2025
- c. IP address 202.163.8.109
- i. Binance User ID ending 9131 accessed on March 26, 2025
 - ii. project575868cn@icloud.com accessed on March 26, 2025
- d. IP address 49.213.18.29
- i. project575868cn@icloud.com accessed on April 16, 2025
 - ii. Binance User ID ending 9131 accessed on April 16, 2025
 - iii. project575868cn@icloud.com accessed on April 23, 2025
 - iv. Binance User ID ending 9131 accessed on April 23, 2025
 - v. zhejiang.cn.110@icloud.com accessed on April 24, 2025
- e. IP address 202.163.8.111
- i. Binance User ID ending 9131 accessed on June 25, 2025
 - ii. Project575868cn@icloud.com accessed on June 25, 2025

63. Upon information and belief, the Defendant Property constitutes proceeds of wire fraud, and property involved in money laundering, all of which is subject to forfeiture to the United States.

64. Upon information and belief, the Defendant Property was involved in concealment money laundering. Criminals often conduct an otherwise unnecessary and costly number of transactions to transfer criminal proceeds via layered transactions designed to conceal or disguise the nature, location, source, ownership, or control of those proceeds. The large number of rapid transfers described above—which have no apparent legitimate purpose—strongly indicate that these funds were transacted in a way designed to conceal or disguise the nature, location, source, ownership, or control of the proceeds of a specified unlawful activity, in this case, wire fraud.

65. The public blockchain analysis in this case, summarized above, demonstrates that the proceeds of the wire fraud scheme were broken up, distributed through a series of virtual currency addresses via rapid transactions, and re-consolidated with other funds in different virtual currency addresses, including Subject Address 1, Subject Address 2, Subject Address 3, and Binance User ID ending 9131.

66. The commission of convoluted, intermingled, and re-consolidated transactions, which incurred transaction fees and served no apparent legitimate purpose, imply that the “purpose of these numerous, fast-repeating, and intermingled transactions was to conceal the nature, source, location, ownership and control of the proceeds.” *See, e.g., United States v. Sterlingov*, No. 1:21-cr-00399-RDM, 2023 WL 2387759, *7 (D.D.C. Mar. 6, 2023) (concluding that “there is probable cause to believe that [defendant’s] seized funds”—even if not proceeds of crime—“were ‘involved in’”

defendant's Bitcoin tumbler business' "unlicensed money transmitting operations" that mixed Bitcoins for a fee, making it more difficult to trace); *United States v. Rodriguez*, 53 F.3d 1439, 1447-48 (7th Cir. 1995) (convoluted real estate transactions, from which intent to conceal or disguise may be inferred, also imply knowledge of illegal source; jury could infer knowledge from combination of suspicion and indifference to the truth).

67. Where it is shown that a suspected money launderer commingled proceeds of specified unlawful activity with untraced funds in an address or wallet via such transactions apparently designed to conceal the nature, source, ownership, location, or control of criminal proceeds, then those commingled untraced funds are forfeitable as having facilitated—and therefore as having been “involved in”—concealment money laundering. *See, e.g., United States v. Bikundi*, 926 F.3d 761, 793-94 (D.C. Cir. 2019) (collecting cases); *see also United States v. Guerrero*, 2021 WL 2550154, *9 (N.D. Ill. June 22, 2021) (money from unknown source that was commingled with fraud proceeds facilitated the concealment laundering of fraud proceeds and, accordingly, property acquired with the commingled funds was forfeitable as property traceable to property involved in a money laundering offense); *United States v. Romano*, 2021 WL 1711633, *5-6 (E.D.N.Y. Apr. 29, 2021) (by laundering fraud proceeds through their personal bank accounts, to commingle the proceeds with other funds for a concealment laundering purpose, the defendants made the commingled funds forfeitable as facilitating property); *United States v. Coffman*, 859 F. Supp. 2d 871, 876-77 (E.D. Ky. 2012) (holding that forfeiture of

legitimate and criminal proceeds commingled in an account is proper as long as the government demonstrates that the defendant pooled the funds to facilitate money laundering by, for example, disguising the nature and source of proceeds; concluding that clean funds in bank account were subject to forfeiture because they had “been co[m]mingled with tainted funds for the purpose of obfuscating the origin or existence of tainted money.”).

68. The transfer of fraud proceeds from multiple victims into the same address or financial account via transactions committed within a relatively short time period strongly indicates that the other funds contained in the address or account are also fraud proceeds and, likewise, that the address or account is being used to collect, conceal, and launder those funds. As shown above, this matter involves such transfers of criminal proceeds into the Subject Addresses.

CLAIM I

69. Plaintiff hereby re-alleges paragraphs 1 – 68, as referenced above.

70. The Defendant Property is forfeitable to the United States pursuant to 18 U.S.C. § 981(a)(1)(A) because it is any property, real or personal, involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956 or any property traceable to such property.

CLAIM II

71. Plaintiff hereby re-alleges paragraphs 1 – 68, as referenced above.

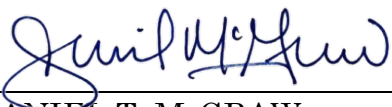
72. The Defendant Property is forfeitable to the United States pursuant to 18 U.S.C. § 981(a)(1)(C) because it is any property, real or personal, which constitutes or is derived from proceeds traceable to wire fraud, in violation of 18 U.S.C. § 1343.

REQUESTED RELIEF

Wherefore, the United States requests that the Court issue a warrant for the arrest of the Defendant Property; that due notice be given to all interested parties to appear and show cause why forfeiture to the United States of America should not be decreed; and that the Defendant Property be condemned and forfeited to the United States of America and be delivered into the custody of the United States Postal Inspection Service or the United States Marshals Service for disposition according to law; and for such other relief as this Court may deem just and proper.

TIMOTHY VERHEY
United States Attorney

Dated: May 13, 2026



DANIEL T. MCGRAW
Assistant United States Attorney
P.O. Box 208
Grand Rapids, Michigan 49501-0208
(616) 456-2404

VERIFICATION

I am a Special Agent with the Federal Bureau of Investigation with personal involvement in this investigation.

I have read the contents of the foregoing Verified Complaint for Forfeiture In Rem, and the statements contained therein are true to the best of my knowledge and belief.

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

Dated: 5/13/2026



TOM PELLER
Special Agent
Federal Bureau of Investigation