UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA **v.** **APPROXIMATELY 1,537,935 USDT** **Defendant, *in rem.***	§ § § § § § § § §	**COMPLAINT FOR FORFEITURE *IN REM*** ***CIVIL ACTION NO.*** **25-cv-3911**

VERIFIED COMPLAINT FOR FORFEITURE *IN REM*

Plaintiff, the United States of America, through the U.S. Attorney for the District of Columbia, brings this verified complaint for forfeiture in a civil action *in rem* against 1,537,935.77125 USDT, hereinafter referred to as "Defendant Property", and alleges as follows:

STATEMENT OF THE CASE

1. Criminals abroad, their associates, and conspirators together stole funds from approximately 95 victims. The funds were then laundered through a convoluted web of cryptocurrency wallets to evade detection and hide the origin of the funds. The Memphis Virtual Currency Task Force (MVCTF), comprised of members from the United States Secret Service (USSS) and Federal Bureau of Investigation (FBI), investigated, traced, and seized the Defendant Property, which constitutes proceeds traceable to those thefts and property involved in, and traceable to, this money laundering scheme.

2. The United States of America seeks to lawfully forfeit the Defendant Property to punish and deter criminal activity by depriving criminals of property used in or acquired through illegal activities, and most importantly, to recover assets that may be used to compensate victims.[1]

[1] *See* United States Asset Forfeiture Program, *Our Mission*, https://www.justice.gov/afp.

JURISDICTION AND VENUE

3. This Court has original jurisdiction of this civil action by virtue of 28 U.S.C. § 1345 because it has been commenced by the United States and by virtue of 28 U.S.C. § 1355(a) because it is an action for the recovery and enforcement of a forfeiture under an Act of Congress.

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

5. Venue is proper in this judicial district under 18 U.S.C. § 3238 and 28 U.S.C. §§ 1355(b) and 1395(a), (b), and (c).

NATURE OF THE ACTION AND STATURY BASIS FOR FORFEITURE

6. The United States files this *in rem* forfeiture action to seek forfeiture of Defendant Property as constituting proceeds of wire fraud and wire fraud conspiracy offenses, committed in violation of 18 U.S.C. §§ 1343, 1349, 2, and 3, and as involved in money laundering and money laundering offenses, committed in violation of 18 U.S.C. 1956(a)(1)(B)(i), 1956(a)(2)(B)(i), 1956(h), and 2, and 3.

7. Procedures for this action are mandated by Rule G of the supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions and, to the extent applicable, 18 U.S.C. §§ 981 and 983 and the Federal Rules of Civil Procedure.

8. 18 U.S.C. § 981(a)(1)(A) mandates forfeiture of any property, real or personal, involved in a transaction or attempted transaction in violation of section 18 U.S.C. §§ 1956, 1957 or 1960, or any property traceable to such property.

9. 18 U.S.C. § 981(a)(1)(C) mandates forfeiture of property constituting or derived from proceeds traceable to wire fraud, conspiracy to commit wire fraud, or any offense constituting "specified unlawful activity" as defined by 18 U.S.C. § 1956(c)(7), or a conspiracy to commit such

offense. A violation of 18 U.S.C. § 1343, or a conspiracy to commit that offense, constitutes specified unlawful activity under 18 U.S.C. § 1956(c)(7)(A) as an offense listed in 18 U.S.C. § 1961(1)(B).

10. 18 U.S.C. § 1343 provides that whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, commits the violation of wire fraud.

11. 18 U.S.C. § 1349 provides that whoever attempts or conspires to commit a violation of 18 U.S.C. § 1343 shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy.

12. 18 U.S.C. § 1956(a)(1)(B)(i) provides in relevant part that whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct 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 specified unlawful activity" is guilty of concealment of money laundering.

13. 18 U.S.C. § 1956(a)(2)(B)(i) provides that whoever transports, transmits, or transfers, or attempts to transport, transmit, or transfer a monetary instrument or funds from a place in the United States to or through a place outside the United States or to a place in the United States from or through a place outside the United States—knowing that the monetary instrument or funds involved in the transportation, transmission, or transfer represent the proceeds of some form of unlawful activity and knowing that such transportation, transmission, or transfer is designed in whole

or in part—to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity, commits international money laundering.

14. 18 U.S.C. § 1956(h) provides that any person who conspires to commit any offense of 1956 or 1957 is subject to the same penalties as those prescribed for the offense the commission of which was the object of the conspiracy.

15. 18 U.S.C.§ 1957 makes it a crime to knowingly engage or attempt to engage in a monetary transaction in criminally derived property of a value greater than $10,000 where those funds are derived from specified unlawful activity.

PROPERTY INFORMATION

16. The Defendant Property is 1,537,935.771225 USDT, which is the equivalent to $1,537,935.77 in USD. The Defendant Property is associated with virtual currency address 0xff928ae4b20c0b9b2f02a4ed99832424991ba89b (the "Subject Virtual Currency Address"), which held 1,537,935.771225 USDT.

17. The currency previously located within the virtual currency address is hereinafter referred to as the "Defendant Property."

18. The Defendant Property is currently in custody and control of the United States Secret Service.

STATEMENT OF FACTS

Background on Cryptocurrency

19. **Virtual Currency**: Virtual currencies are digital representations of value that, like traditional coin and paper currency, function as a medium of exchange (i.e., they can be digitally traded or transferred and can be used for payment or investment purposes). Virtual currencies are a type of digital asset separate and distinct from digital representations of traditional currencies, securities, and other traditional financial assets. The exchange value of a particular virtual currency generally is based on agreement or trust among its community of users. Some virtual currencies have equivalent values in real currency or can act as a substitute for real currency, while others are specific to particular virtual domains (e.g., online gaming communities) and generally cannot be exchanged for real currency. Cryptocurrencies, like Bitcoin (or BTC) and Ether (or ETH), are types of virtual currencies, which rely on cryptography for security. Cryptocurrencies typically lack a central administrator to issue the currency and maintain payment ledgers. Instead, cryptocurrencies use algorithms, a distributed ledger known as a blockchain, and a network of peer-to-peer users to maintain an accurate system of payments and receipts.

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

21. **Blockchain Analysis**: Law enforcement can trace transactions on blockchains to determine which virtual currency addresses are sending and receiving particular virtual currency. This analysis can be invaluable to criminal investigations for many reasons, including that it may enable law enforcement to uncover transactions involving illicit funds and to identify the person(s) behind those transactions. To conduct blockchain analysis, law enforcement officers use reputable, free open source blockchain explorers, as well as commercial tools and services. These commercial tools are offered by different blockchain-analysis companies. Through numerous unrelated investigations, law enforcement has found the information associated with these tools to be reliable.

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

23. **Virtual Currency Exchange**: A virtual currency exchange ("VCE"), also called a cryptocurrency exchange, is a platform used to buy and sell virtual currencies. VCEs allow users to exchange their virtual currency for other virtual currencies or fiat currency, and vice versa. Many VCEs also store their customers' virtual currency addresses in hosted wallets. VCEs can be centralized (i.e., an entity or organization that facilitates virtual currency trading between parties on a large scale and often resembles traditional asset exchanges like the exchange of stocks) or decentralized (i.e., a peer-to-peer marketplace where transactions occur directly between parties).

24. **Virtual Currency Wallet**: A virtual currency wallet (e.g., a hardware wallet, software wallet, or paper wallet) stores a user's public and private keys, allowing a user to send and receive virtual currency stored on the blockchain. Multiple virtual currency addresses can be controlled by one wallet.

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

26. **Transaction Fee**: A transaction fee is a fee paid by the party sending virtual currency on a blockchain to reward miners and/or validators for verifying and validating transactions. Transaction fees vary by blockchain and can fluctuate based on factors such as blockchain network traffic and transaction sizes. Senders of virtual currency can increase the transaction fees that they pay to have their transactions confirmed faster by miners and/or validators. Transaction fees are generally paid in a blockchain's native token (e.g., Bitcoin on the Bitcoin blockchain). On the Ethereum network, these transaction fees are called "gas fees."

27. **Ethereum:** Ether ("ETH") is a cryptocurrency that is open source, public, has a blockchain, and is distributed on a platform that uses "smart contract" technology. The public ledger is the digital trail of the Ethereum blockchain, which allows anyone to track the movement of ETH.

28. **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, Tether tokens (also known as 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.

29. **USDT and Tether Limited:** Tether Limited ("Tether") is a company that manages the smart contracts and the treasury (*i.e.*, the funds held in reserve) for USDT tokens.

30. Like other virtual currencies, USDT is sent to and received from USDT "addresses." A USDT address is somewhat analogous to a bank account number and is represented as a 46 to 48-character-long case-sensitive string of letters and numbers. Users can operate multiple USDT addresses at any given time, with the possibility of using a unique USDT address for every transaction.

31. Although the identity of a USDT 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 USDT address. The analysis can also, in some instances, reveal additional addresses controlled by the same individual or entity.

32. **Smart Contracts**: Smart contracts allow developers to create markets, store registries of debts, and move funds in accordance with the instructions provided in the contract's code, without any type of middleman or counterparty controlling a desired or politically motivated outcome, all while using the Ethereum blockchain protocol to maintain transparency. Smart contract technology is one of Ethereum's distinguishing characteristics and an important tool for companies or individuals executing trades on the Ethereum blockchain. When engaged, smart contracts automatically execute according to the terms of the contract written into lines of code. A transaction contemplated by a smart contract occurs on the Ethereum blockchain and is both trackable and irreversible.

33. **Gas Fees:** Transfers of cryptocurrencies are subject to transaction costs. Each blockchain maintains its own manner of paying those costs. Transactions, including transfers conducted on the Ethereum blockchain, incur costs known as "Gas" or Gas fees. Gas fees are transaction costs which must be paid in Ether, or its fraction, gwei, the native cryptocurrency of the Ethereum network. These fees serve as a form of remuneration for validators who maintain and secure the network. Gas fees fluctuate based on supply, demand, and network capacity, and may increase during periods of network congestion. Users pay these Gas fees to third parties, called miners, who engage with the Ethereum ecosystem in an effort to support the transfer of cryptocurrencies worldwide. This includes transactions involving Ethereum network tokens, such as USDT and USDC, whose outgoing transfers would each require Gas fees to be paid in ETH and cannot be paid using tokens. Therefore, a wallet address would need an ETH balance to initiate sending a transaction.

34. Due to the nature of Gas fees, it is common that the payor of the fees is associated with or the owner or individual manager of a particular address who is attempting to initiate the transaction. A simplified analogy is mailing a letter through the U.S. Mail. The postage cost is like the Gas fee in Ethereum. Just as an individual must pay the postage to send a letter, an individual transacting on the Ethereum network must pay a Gas fee. Moreover, given that a letter is sent using postage that a sender commonly pays for, the postage can be presumed to be sent or associated with the mailer. The same logic holds in cryptocurrency transactions, where transferors typically pay fees associated with transfers. With Gas fees, however, the postage is more like a digital fingerprint, in that it cannot be changed or manipulated in any way.

35. Investigators may be able to trace Gas fee payments, and that tracing may provide evidence as to the ownership or control of the underlying transaction.

Background on Cryptocurrency Confidence Scams

36. Cryptocurrency confidence scams, commonly known as "Pig Butchering," are a type of internet-based cryptocurrency investment scam. The phrase is translated from Chinese shāzhūpán and refers to a scam in which the victim is "fattened up prior to slaughter." These scams are also referred to as cryptocurrency investment fraud.[2] These types of scams typically involved four stages. First, a perpetrator cold contacts a victim via text, social media, or some other communication platform. Oftentimes, the perpetrator will pretend to have contacted the wrong number but continue communicating with their newfound "friend." Second, the perpetrator will establish a relationship with the victim by continuing to message them over days, weeks, or months. Third, the scammer will concoct a narrative to induce the victim to send them a series of purported investments, often in the form of cryptocurrency. These payments are often made through fraudulent investment platforms introduced by the scammer, which the victim believes to be legitimate. Fourth, after the victim stops sending additional payments, or begins to question the scammer about legitimacy of their "investments," the perpetrator cuts off all contact.

37. Confidence schemes are schemes where perpetrators gain trust or confidence from victims to deceive them into parting with their money. One of the most well-known forms of confidence schemes is the "romance scam," which typically features a perpetrator befriending a victim through the guise of a romantic relationship, often solely existing online, in an effort to siphon funds from the victim's bank accounts or assets.

38. Cryptocurrency confidence scams feature elements of well-established investment schemes blended with fraudulent websites, or mobile apps, and the complexity of cryptocurrency.

[2] Federal Bureau of Investigation, *Cryptocurrency Investment Fraud,* https://www.fbi.gov/how-we-can-help-you/victim-services/national-crimes-and-victim-resources/cryptocurrency-investment-fraud?__cf_chl_rt_tk=KP0jo5lKxpcHNmC2W9IgFvxzVp58YptXkC36h1AH84I-1749423762-1.0.1.1-PrqYwbOk3o56Boyjv4_oSFvOb0GH2RnyJMQVGilzVSs (Last accessed Jun. 17, 2025).

39. Law enforcement and independent investigations have determined that these schemes are perpetrated primarily in Southeast Asia, often via forced labor. Victims are trafficked into countries that include Myanmar, Philippines, Laos and Cambodia and are forced to conduct these scams via text messages, dating websites, and other online platforms inside scam compounds in these countries.[3]

40. Confidence schemes, or romance scams, were reported to have cost U.S. victims $238 million in losses in 2018, $375 million in losses in 2019, and over $600 million in losses in 2020. Separately, during this same time-period, investment scams were reported to have cost U.S. victims over $800 million dollars.[4]

41. After the emergence of cryptocurrency-based confidence scams in 2020, losses in those same scam categories have jumped to reported losses of over $5.22 billion in 2023 and approximately $7 billion in 2024.[5] In 2024, approximately $5.8 billion in losses from cryptocurrency investment fraud was reported to the Internet Crime Complaint Center.[6]

42. Cryptocurrency investment fraud frequently involves use of smartphone applications. Ninety-seven percent of Americans own a cellphone of some kind and nine-in-ten own a smartphone.[7]

---

[3] Cezary Podkul and Cindy Liu, *Human Trafficking's Newest Abuse: Forcing Victims into Cyberscamming*, https://www.propublica.org/article/human-traffickers-force-victims-into-cyberscamming, (Sept. 13, 2022).
[4] Federal Bureau of Investigation Internet Crime Complaint Center, *Internet Crime Report 2020*, https://www.ic3.gov/AnnualReport/Reports/2020_ic3report.pdf, (Mar. 17, 2021).
[5] Federal Bureau of Investigation Internet Computer Complaint Center, *Internet Crime Report 2024,* https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf, (Apr. 23, 2025).
[6] *Id.*
[7] Eugenie Park, Kaitlyn Radde, Michelle Faverio, Olivia Sidoti, Risa Gelles-Watnick, Sara Atske and Wyatt Dawson, *Mobile Fact Sheet,* https://www.pewresearch.org/internet/fact-sheet/mobile/ (Nov. 13, 2024).

43. Types of apps available on smartphones include mobile banking or investment apps, which are typically associated with an individual's bank or investment account. These apps typically display an account owner's balance and transaction history, among other information. Notably, as of 2022, nearly 80% of Americans regularly used mobile banking apps or websites.[8]

44. This trust in mobile banking and investment apps is at the center of these schemes. Following the initial victimization through the confidence scheme, perpetrators convince victims to download what appear to be legitimate mobile banking or investment apps to track their cryptocurrency investments. In reality, the apps are not connected to any real account or legitimate financial institution. Instead, the apps are created and controlled by the perpetrators, who are able to create the facade of balances and transactions that are otherwise non-existent.

45. This fabricated activity, which on the surface would appear no different than that of a legitimate mobile banking or investment app, is made to appear as though investments into non-existent or perpetrator-controlled platforms are realizing substantial gains. This helps the perpetrators convince victims into investing additional funds into the scheme.

46. Victims may contribute a small amount of funds to a cryptocurrency confidence scam, unwittingly, only to see those funds appear to triple in value, as displayed on the perpetrator-controlled app. Some victims then attempt to invest more assets, which may include IRAs, 401(k)s, home equity loans, and college savings plans.

[8] American Bankers Association, *National Survey: Record Number of Bank Customers Use Mobile Apps More Than Any Other Channel to Manage Their Accounts,* https://www.aba.com/about-us/press-room/press-releases/consumer-survey-banking-methods-2024#:~:text=The%20national%20survey%20found%20that,in%20the%20past%2012%20months. (Nov. 22, 2024).

47. Some victims report being able initially to successfully withdraw funds, thinking they are gains, which leads to the victims placing more trust and credibility with the perpetrators. This stage in the fraud scheme is designed to give the victims more confidence to invest their remaining assets. In reality, these victims likely withdraw funds deducted from their "investments" (rather than purported gains), or originating from other victims.

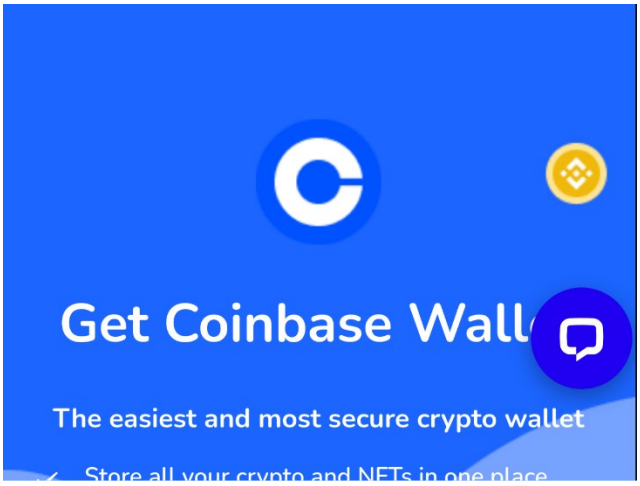
48. Cryptocurrency confidence schemes most often involve cryptocurrency at the center of the investments. Cryptocurrency is often perceived as a highly volatile asset, with price swings fluctuating the value of some cryptocurrencies, like Bitcoin, thousands of dollars in any given day. Cryptocurrency can also be highly technical, with terminology and attributes unique to different cryptocurrencies and blockchains. This has allowed for perpetrators to help convincingly explain convoluted cryptocurrency related investments to victims that otherwise would not consider purchasing or investing in cryptocurrency.

Wire Fraud Scheme

49. Victim-1 in September 2024 reported that they were a victim of a cryptocurrency investment scam and lost over $600,000.

50. In or around July 2024, Victim-1 received and accepted a friend request from an individual, hereafter known as "Scammer-1" on an online dating platform called "Hinge." Victim-1 reported that shortly after his/her initial contact, Scammer-1 requested Victim-1 to consider investing in cryptocurrency and provided a purported investment website to Victim-1. The website, contractmarket-app.com, displayed logos that resembled logos from the actual website of Coinbase, a well-known and legitimate cryptocurrency exchange (as shown in Exhibit 1 below). MVCTF reviewed the site and confirmed that the website was not a legitimate cryptocurrency investment site and was indeed a spoofed version of the Coinbase platform. This is typical in cryptocurrency confidence scams; the threat actors will provide a URL or QR code to the victims, which takes the victim to a website controlled by the threat actors that mimics legitimate cryptocurrency trading platforms. This allows the threat actors to show fraudulent and inflated investment gains through their website, which is made to look like a legitimate exchange website.

Exhibit 1 – Logo on Fraudulent Investment Website



51. Subsequently, Victim-1 accessed contractmarket-app.com, still believing it to be a legitimate investment website, and started "investing" small amounts (such as $1,000-$2,000) believing he/she was making returns on his/her funds.

52. Scammer-1 then "loaned" $300,000 worth of "coins" to Victim-1 by purporting to deposit funds into the victim's contractmarket-app.com account in order to convince Victim-1 to invest more money through contractmarket-app.com. Often, threat actors will purport to "loan" the victim funds directly into their investment accounts to help their investment portfolio, when in fact, the amount of the investment is not increasing. Victim-1 then deposited $150,000 worth of Victim-1's own funds. Shortly after, contractmarket-app.com revealed that the $150,000 investment quickly turned into $1,300,000 in an unspecified cryptocurrency.

53. When Victim-1 decided that it was time to start cashing out some of his/her profits, Victim-1 was unable to do so. In or around August 2024, Victim-1 attempted to withdraw the funds, but received an error message. The message stated that the $300,000 loaned to Victim-1 received was associated with money laundering. Victim-1 was advised by purported customer service representatives on contractmarket-app.com that he/she needed to deposit $300,000 to resolve this issue. As a result, Victim-1 deposited $300,000 of his/her money into the scam website, contractmarket-app.com. This additional $300,000 raised the purported value in the victim's account on the fraudulent investment website to $1,600,000. Victim-1 then tried to withdraw his/her funds again from contractmarket-app.com but failed.

54. At that point, Victim-1 was advised by Scammer-1 that an additional $180,000 in taxes needed to be paid to receive the funds back. Victim-1 thought he/she had no choice, so Victim-1 sold legitimate investments to pay another $180,000 to the scam website. This brought his/her total amount deposited to approximately $615,424, not including the funds supposedly "loaned" by the scammer or his/her supposed profit. Assuming this would resolve the issue, Victim-1 attempted to withdraw his/her funds again but was told that he/she had to pay another payment of $160,000. At this point, Victim-1 realized he/she had been scammed and had lost the total amount of approximately $615,424.

55. Victim-1 advised investigators he/she deposited about $176,545 worth of USDT of their "invested" funds from his/her Coinbase account to 0x771367759065208a8547a1f633cb887365c7580f ("Scam Address 580f"), an address provided by the contractmarket-app.com customer service representatives. Investigators traced $100,000 worth of USDT of Victim-1's funds from Scam Address 580f through two other unhosted addresses and ultimately to the **SUBJECT VIRTUAL CURRENCY ADDRESS**, where those funds remained until they were seized by law enforcement (as represented in Exhibit 2 below). The transfer of funds from the initial scam address to the **SUBJECT VIRTUAL CURRENCY ADDRESS** occurred over the course of less than 24 hours.

Exhibit 2 – Summary flow of funds from Victim-1 to SUBJECT VIRTUAL CURRENCY ADDRESS

The Movement of Other Funds from Scam Address 580f to SUBJECT VIRTUAL CURRENCY ADDRESS

56. Investigators identified approximately 91 addresses involved in the movement of funds that were ultimately deposited into the **SUBJECT VIRTUAL CURRENCY ADDRESS**. These 91 addresses operated as intermediary addresses—which are unhosted addresses through which the funds passed on their way to their ultimate destination, in this case, the **SUBJECT VIRTUAL CURRENCY ADDRESS**.

57. Through blockchain tracing, investigators analyzed the flow of funds from Scam Address 580f to the **SUBJECT VIRTUAL CURRENCY ADDRESS** between on or about June 14, 2024, and August 27, 2024, which revealed several unique indicators suggesting the funds originated from Cryptocurrency Confidence Scams or other fraudulent activity. For instance:

i. All of the intermediary addresses used to funnel funds from Scam Address 580f to **SUBJECT VIRTUAL CURRENCY ADDRESS** were established between in or around June 2024 to in or around August 2024, which is the same timeframe as when Victim-1 was scammed.

ii. The intermediary addresses exhibited large dollar deposit transactions, followed by a pattern of rapid movement of funds with large corresponding withdrawals. During the short time period between in or around June 2024 to in or around August 2024, the intermediary addresses each processed an average of approximately $25 million of cryptocurrency.

iii. Five of the intermediary addresses received and sent transactions that were worth over $100 million in total from in or around June 2024 through in or around August 2024. Two other intermediary addresses that the MVCTF analyzed received and processed approximately $400 million of cryptocurrency in just twelve months. These two

intermediary addresses interacted directly with the **SUBJECT VIRTUAL CURRENCY ADDRESS** and have sent a combined $2.5 million to the **SUBJECT VIRTUAL CURRENCY ADDRESS** from in or around June 2024 to in or around August 2024.

58. Criminals will often conduct multiple unnecessary and costly 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. Each transaction between addresses requires a gas fee; the sender therefore loses money each time they send to additional addresses. The large number of rapid transfers—with no apparent legitimate purpose—from the intermediary addresses to **SUBJECT VIRTUAL CURRENCY ADDRESS** 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 (in this case, wire fraud).

Additional Victim Proceeds Traced to SUBJECT VIRTUAL CURRENCY ADDRESS

59. Investigators identified and confirmed five additional victims[9] who in or around June 2024 to in or around August 2024 sent a combined amount of approximately $4 million to a group of addresses designated by a reliable blockchain tracing tool as, "Pig Butchering Group 26" (0xf0473f9797d2ebd2998764468fc8e90b1c0fbc01).[10] This group of addresses sent approximately $100,000 of these victim funds through five separate addresses within the span of seven days, ultimately depositing the victim funds in the **SUBJECT VIRTUAL CURRENCY ADDRESS**. The approximately $100,000 in victim funds were held in **SUBJECT VIRTUAL CURRENCY ADDRESS** at the time of seizure.

60. Through victim reports to the U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN"), IC3.gov, and to four virtual currency exchanges, and additional backtracing from addresses provided by victims who were defrauded, investigators identified another 85 victims who sent a combined amount of approximately $29.85 million to addresses associated with a fraudulent domain called "cp-berage.top," which is known to law enforcement as a fraudulent cryptocurrency investment website. Approximately $139,930 of the victim funds sent to an address associated with the fraudulent domain "cp-berage.top" were then laundered through nine separate addresses and then were sent to the **SUBJECT VIRTUAL CURRENCY ADDRESS** as shown in the chart below. Of the $139,930 worth of cryptocurrency in known victim funds, $90,000 were still held in **SUBJECT VIRTUAL CURRENCY ADDRESS** at the time of seizure.

[9] Two victims submitted reports to law enforcement on IC3.gov, reporting being scammed and sending funds to the addresses discussed in this paragraph. Three other victims sent funds from virtual currency exchanges to the addresses discussed in this paragraph and submitted fraud reports to those exchanges identifying that they had been scammed and that the addresses they sent funds to were fraudulent.

[10] A blockchain tracing tool used by law enforcement sometimes labels clusters of wallet addresses based on information provided by victims, non-profits that represent victims, or other reporting suggesting the wallet address is tied to fraudulent activity. While law enforcement does not rely on such designations without examining source material, they provide additional evidence that the address has received likely fraudulent funds.

Tracing Funds from Scam Addresses to the SUBJECT VIRTUAL CURRENCY ADDRESS

61. Investigators also identified approximately 120 additional suspected[11] victims whose funds were sent from initial deposit addresses to the **SUBJECT VIRTUAL CURRENCY ADDRESS**, where their funds remained as of the date of the seizure. In total, investigators have traced approximately $430,148 of victim funds—including—Victim-1's funds, following a similar pattern described above, into **SUBJECT VIRTUAL CURRENCY ADDRESS**.

[11] Determinations that senders are suspected victims are based on flows from exchanges that have the same pattern of movement through various intermediary wallets as confirmed victims flows that are laundered to the target addresses.

VICTIM LOSS SUMMARY

62. As shown below in Exhibit 3, through blockchain tracing and additional investigation, investigators have determined that of victims lost a total of approximately $37,005,534. This does not include the suspected victim funds described in paragraph 61.

Exhibit 3 – Total Loss Summary

Victim	Approx. Total Loss Amount
Victim 1	$615,424
Victim 2	$2,400,000
Victim 3	$139,930
Victims 4-8	$4,000,000
Victims 9-93	$29,850,000
Total	**$37,005,354.00**

COUNT ONE – FORFEITURE OF DEFENDANT PROPERTY

(18 U.S.C. § 981(a)(1)(C))

63. The Defendant Property includes property constituting or derived from proceeds traceable to wire fraud and conspiracy to commit wire fraud, in violation of 18 U.S.C. §§ 1343 and 1349.

64. Accordingly, the Defendant Property is subject to forfeiture to the United States under 18 U.S.C. § 981(a)(1)(C).

COUNT TWO – FORFEITURE OF DEFENDANT PROPERTY

(18 U.S.C. § 981(a)(1)(A))

65. The Defendant Property constitutes property involved (a) domestic and international concealment of money laundering transactions committed in violation of Title 18, United States Code, Sections 1956(a)(1)(B)(i) and 1956(a)(2)(B)(i), (b) a conspiracy to engage in money laundering, committed in violation of Title 18, United States Code, Section 1956(h), and (c) violations of Title 18, United States Code, Sections 1957.

66. Accordingly, the Defendant Funds are subject to forfeiture to the United States under 18 U.S.C. § 981(a)(1)(A).

PRAYER FOR RELIEF

WHEREFORE, the United States of America prays that notice issue on the Defendant Property as described above; that due notice be given to all parties to appear and show cause why the forfeiture should not be decreed; that this Honorable Court issue a warrant of arrest *in rem* according to law; that judgment be entered declaring that the Defendant Property be forfeited to the United States of America for disposition according to law; and that the United States of America be granted such other relief as this Court may deem just and proper.

Respectfully submitted,

JEANINE FERRIS PIRRO
United States Attorney

By: /s/ Rick Blaylock Jr.
RICK BLAYLOCK JR.
Assistant United States Attorney
Asset Forfeiture Coordinator
Texas Bar Number 24103294
United States Attorney's Office
601 D Street NW
Washington, D.C. 20530
Telephone: 202-252-6765
Email: rick.blaylock.jr@usdoj.gov

VERIFICATION

I, Morgan Morgan, a Special Agent with the United States Secret Service, declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the foregoing Verified Complaint for Forfeiture *in rem* is based upon reports and information known to me and/or furnished to me by other law enforcement representatives and that everything represented herein is true and correct.

Executed on this 12th day of November, 2025.

Morgan Morgan
Special Agent
United States Secret Service