

Insult To Injury - "You're a Good Pig, Just Not Fat Enough"



S.W. (not his real name) thought he was having a lucky day when a woman named Kristina Tian reached out on LinkedIn in July 2024. The investment professional from “Mucker Capital” seemed genuinely interested in discussing market strategies.

What S.W. didn't know was that "Kristina" was actually part of an international criminal network operating from Southeast Asia. And he was about to get conned out of his life savings.

A Well-Used Script Played Out

The relationship followed a carefully choreographed script. After their initial LinkedIn exchange, Kristina suggested they move to WhatsApp for more personal conversations. She shared stories about her investment successes and gradually steered discussions toward investment.

She eventually got S.W. to go to a website to deposit some money. The website looked professional, complete with real-time trading data and impressive return charts.

S.W. converted approximately \$500,000 of his money into Ethereum and transferred it to what he believed was Coinbase wallet address recommended by Kristina.

By the end of July, S.W. had invested his \$500,000 and was planning to add another \$200,000 to his portfolio. The fake platform showed returns for his initial investment that far exceeded his expectations.

He Got A Call From The FBI

On July 30, 2024, S.W.'s phone rang with a call that would change everything. FBI agents, working an ongoing investigation into cryptocurrency fraud, had identified him as a potential victim. They were calling to warn him before he lost more money.

He Confronted Kristina And She Called Him A Pig

After receiving the FBI warning, S.W. confronted Kristina via WhatsApp. And that is when Kristina turned into a raging asshole.

Over the course of ten minutes, the person he'd trusted sent messages showing their complete contempt for him.

Here are some of those messages:

4:11 PM: "I feel for you."

4:12 PM: "You're a good pig, just not fat enough."

4:13 PM: "But thank you for giving me half of your savings."

4:20 PM: "Lol, I enjoyed it, and thank you for the money so I can find more."

4:20 PM: "🤔"

4:20 PM: "Glad to use your life savings."

The messages revealed that these scammers really don't care about anyone. It's likely that the WhatsApp messages were not the original person that scammed him, but a manager.

Usually when a victim confronts the scammer, the bosses step in and take over.

Will He Get The Last Laugh, The FBI Froze Over \$500,000 In Funds

As it turns out, the FBI was on the case. The cryptocurrency trail led through a maze of addresses and transactions.

By September 6, 2024, investigators tracked S.W.'s funds as they were converted to Tether (USDT) cryptocurrency and moved to the Tron blockchain. The money eventually landed in an address that contained approximately \$501,595 worth of stolen funds.

On September 8, 2024, Tether Limited froze the criminal address containing S.W.'s funds. By November 5, federal authorities had obtained seizure warrants and recovered approximately \$680,000 in stolen cryptocurrency from two addresses connected to the scheme.

It's unclear if he will get the money back, but one good thing is that the Pig Butchering bosses won't get it!

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

| | | |
|--------------------------------------|---|--------------------------------|
| UNITED STATES OF AMERICA, |) | CASE NO. |
| |) | |
| Plaintiff, |) | |
| |) | JUDGE |
| v. |) | |
| |) | |
| 501,595.10 TETHER (“USDT”) |) | |
| CRYPTOCURRENCY, VALUED AT |) | |
| APPROXIMATELY \$501,595.10, FORMERLY |) | |
| ASSOCIATED WITH CRYPTOCURRENCY |) | |
| ADDRESS BEGINNING/ENDING |) | |
| TGZdF . . . mYHyPDF, and |) | |
| |) | |
| 178,386.12 TETHER (“USDT”) |) | |
| CRYPTOCURRENCY, VALUED AT |) | |
| APPROXIMATELY \$178,386.12, FORMERLY |) | |
| ASSOCIATED WITH CRYPTOCURRENCY |) | |
| ADDRESS BEGINNING/ENDING |) | |
| THr7k . . . q9gskdN, |) | |
| |) | |
| Defendants. |) | COMPLAINT IN FORFEITURE |

NOW COMES plaintiff, the United States of America, by its attorneys, Carol M. Skutnik, Acting United States Attorney for the Northern District of Ohio, and James L. Morford, Assistant U.S. Attorney, and files this Complaint in Forfeiture, respectfully alleging on information and belief as follows in accordance with Supplemental Rule G(2) of the Federal Rules of Civil Procedure:

I. *JURISDICTION AND INTRODUCTION.*

1. This Court has subject matter jurisdiction over an action commenced by the United States under 28 U.S.C. Section 1345, and over an action for forfeiture under 28 U.S.C.

Section 1355(a). This Court also has jurisdiction over this particular action under 18 U.S.C. Section 981(a)(1)(C) (civil forfeiture authority: wire fraud/conspiracy) and 18 U.S.C. Section 981(a)(1)(A) (civil forfeiture authority: money laundering).

2. This Court has *in rem* jurisdiction over the defendant properties pursuant to: (i) 28 U.S.C. Section 1355(b)(1)(A) because acts giving rise to the forfeiture occurred in this district; and, (ii) 28 U.S.C. Section 1355(b)(1)(B), incorporating 28 U.S.C. Section 1395, because the action accrued in this district.

3. The defendant properties are presently in the custody of the United States Marshals Service (USMS). This Court will have control over the defendant properties through service of arrest warrant(s) *in rem*, which the USMS will execute upon the defendant properties. *See*, Supplemental Rules G(3)(b) and G(3)(c).

4. Venue is proper in this district pursuant to: (i) 28 U.S.C. Section 1355(b)(1)(A) because acts giving rise to the forfeiture occurred in this district; and, (ii) 28 U.S.C. Section 1395 because the action accrued in this district.

5. The defendant properties are subject to forfeiture to the United States under 18 U.S.C. Section 981(a)(1)(C) as property which constitutes, or is derived from, proceeds traceable to an offense(s) constituting “specified unlawful activity” (SUA) - as defined in 18 U.S.C. Section 1956(c)(7), with reference to 18 U.S.C. Section 1961(l) - namely: wire fraud, in violation of 18 U.S.C. Section 1343, and wire fraud conspiracy, in violation of 18 U.S.C. Section 371.

6. The defendant properties also are subject to forfeiture to the United States under 18 U.S.C. Section 981(a)(1)(A) as property that was involved in a transaction(s) - or attempted transaction(s) - in violation of 18 U.S.C. Section 1957 (sometimes referred to as transactional

money laundering) and/or 18 U.S.C. Section 1956(a)(1)(B)(i) (sometimes referred to as concealment money laundering), or as property traceable to such property.

II. *DESCRIPTION OF THE DEFENDANT PROPERTIES.*

7. The following properties are the defendant properties in the instant case:

a.) 501,595.10 Tether (“USDT”) cryptocurrency, valued at approximately \$501,595.10, formerly associated with the cryptocurrency address beginning/ending TGZdF . . . mYHyPDF on the Tron blockchain. On or about September 8, 2024, the USDT tokens at the cryptocurrency address were frozen by Tether Limited Inc. (“Tether Limited”). Thereafter, pursuant to a federal seizure warrant issued by U.S. Magistrate Judge James E. Grimes, Jr., on November 5, 2024, Tether Limited “burned” the USDT tokens associated with the cryptocurrency address and reissued the equivalent amount of USDT tokens [namely, 501,595.10 USDT] to a U.S. law enforcement-controlled virtual currency wallet. The cryptocurrency address beginning/ending TGZdF . . . mYHyPDF is referred to in the following paragraphs as **“ADDRESS-12.”**

b.) 178,386.12 Tether (“USDT”) cryptocurrency, valued at approximately \$178,386.12, formerly associated with the cryptocurrency address beginning/ending THr7k . . . q9gskdN on the Tron blockchain. On or about October 16, 2024, the USDT tokens at the cryptocurrency address were frozen by Tether Limited Inc. (“Tether Limited”). Thereafter, pursuant to a federal seizure warrant issued by U.S. Magistrate Judge James E. Grimes, Jr., on November 5, 2024, Tether Limited “burned” the USDT tokens associated with the cryptocurrency address and reissued the equivalent amount of USDT tokens [namely, 178,386.12 USDT] to a U.S. law enforcement-controlled virtual currency wallet. The cryptocurrency

address beginning/ending THr7k . . . q9gskdN is referred to in the following paragraphs as
“ADDRESS-17.”

III. *STATUTES.*

8. *Offense Statutes.* This Complaint in Forfeiture relates to violations of 18 U.S.C. Section 1343 (wire fraud), 18 U.S.C. Section 371 (wire fraud conspiracy), and 18 U.S.C. Sections 1957 and 1956 (money laundering).

9. *Wire fraud:* 18 U.S.C. Section 1343 makes it a crime for anyone, 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, to transmit or cause to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice.

10. *Money Laundering [§ 1957]:* 18 U.S.C. Section 1957 prohibits an individual from engaging or attempting to engage “in a monetary transaction in criminally derived property of a value greater than \$10,000.00 and derived from specified unlawful activity.”

11. *Money Laundering [§ 1956(a)(1)(B)(i)]:* 18 U.S.C. Section 1956(a)(1)(B)(i) makes it a crime to conduct or attempt to conduct “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.”

12. *Forfeiture Statutes:*

a.) *Wire Fraud:* Under 18 U.S.C. Section 981(a)(1)(C), any property - real or personal - which constitutes or is derived from proceeds traceable to a violation of 18 U.S.C.

Section 1343 (wire fraud), or a conspiracy to commit such offense, is subject to forfeiture.

b.) *Money Laundering:* Under 18 U.S.C. Section 981(a)(1)(A), any property - real or personal - “involved in” or traceable to an offense in violation of 18 U.S.C. Section 1957 (transactional money laundering) and/or 18 U.S.C. Section 1956(a)(1)(B)(i) (concealment money laundering) is subject to forfeiture.

13. Particularly, under a money laundering theory of forfeiture, the government is not limited to forfeiting only the criminal proceeds involved in the money laundering transaction. Rather, the government may also forfeit “other funds” involved in the money laundering transaction where those funds were part of the corpus of the laundering transaction or where those “other funds” facilitated the money laundering transaction.

14. *“Corpus” of the Laundering Transaction:* Where the financial transaction is a transfer of a commingled sum of money from cryptocurrency address A to address B, if that transaction constituted a money laundering transaction, then the entire sum transferred is forfeitable as the corpus of the money laundering offense. The SUA proceeds involved in the financial transaction - as well as any “other funds” transferred with it - constitute the corpus of the money laundering transaction; both are subject to forfeiture.

15. *Facilitation of a Laundering Transaction:* “Other funds” that facilitate the money laundering conduct - by helping conceal the nature, source, ownership, or control of the cryptocurrency traceable to a fraud victim - are likewise subject to forfeiture. For example, “other funds” transferred with the SUA proceeds as part of a concealment money laundering offense are subject to forfeiture as property “involved in” the offense. The “other funds” commingled with the SUA proceeds obfuscate the origin or existence of the SUA proceeds.

IV. *BACKGROUND ON CRYPTOCURRENCY.*

16. *Virtual Currency:* Virtual currencies are digital tokens of value circulated over the internet. Virtual currencies are typically not issued by any government or bank like traditional fiat currencies, such as the U.S. Dollar, but rather are generated and controlled through computer software. Different virtual currencies operate on different blockchains, and there are many different, widely used virtual currencies currently in circulation. Bitcoin (or BTC) and Ether (ETH) are currently the most well-known virtual currencies in use. BTC exists on the BTC blockchain and ETH exists on the Ethereum network.

17. *DAI:* DAI (“DAI”) is a decentralized “stablecoin,” a type of blockchain-based virtual currency that is tied - or tethered - to a fiat currency. DAI exists on the Ethereum blockchain. The issuance of DAI is controlled by smart contracts and DAI is backed by overcollateralized loans. DAI is intended to represent the U.S. Dollar at a 1:1 ratio.

18. *Tether:* Tether (“USDT”) is a “stablecoin,” a type of blockchain-based virtual currency that is tied - or tethered - to a fiat currency. USDT exists on several third-party blockchains, including Ethereum. USDT is a centralized stablecoin, which means the cryptocurrency is backed by U.S. Dollars and other assets held by Tether Limited. Tether Limited is a company that manages the smart contracts and the treasury (*i.e.*, the funds held in reserve) for USDT tokens. Tether seeks to peg USDT to the U.S. Dollar at a 1:1 ratio.

19. *Virtual Currency Address:* 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 letters and numbers.

20. *Private Key:* Each virtual currency address is controlled using a unique corresponding private key, a cryptographic equivalent of a password, which is needed to access

the address. Only the holder(s) of an address' private key can authorize a transfer of virtual currency from that address to another address.

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

22. *Hosted Wallets:* Wallets that are hosted by third parties are referred to as "hosted wallets" because the third party retains a customer's funds until the customer is ready to transact with those funds.

23. *Virtual Currency Exchanges ("VCEs"):* VCEs are trading and/or storage platforms for virtual currencies. Many VCEs also store their customers' virtual currency in virtual currency wallets. Because VCEs act as money services businesses, they are legally required to conduct due diligence of their customers (*i.e.*, Know Your Customer - "KYC" - checks) and to have anti-money laundering programs in place to the extent they operate and service customers in the United States.

24. *Unhosted Wallets:* An "unhosted wallet", also known as cold storage or self-custody, is a cryptocurrency wallet that is not hosted or controlled by a cryptocurrency exchange. Unhosted wallets allow users to exercise total, independent control over their funds.

25. *Blockchain:* Many virtual currencies publicly record all of their transactions on what is known as a blockchain. The blockchain is essentially a distributed public ledger, run by the decentralized network of computers, containing an immutable and historical record of every

transaction utilizing that blockchain's technology. The blockchain can be updated multiple times per hour; it records every virtual currency address that has ever received virtual currency and maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies.

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

27. API stands for application programming interface, which is a set of definitions and protocols for building and integrating application software.

28. For all cryptocurrency transactions detailed herein, dates, times, amounts, and valuations are all approximations.

V. *BACKGROUND OF INVESTIGATION.*

29. The FBI Cleveland Field Office has investigated cryptocurrency confidence fraud scams perpetrated on victims throughout the United States, including in the Northern District of Ohio.

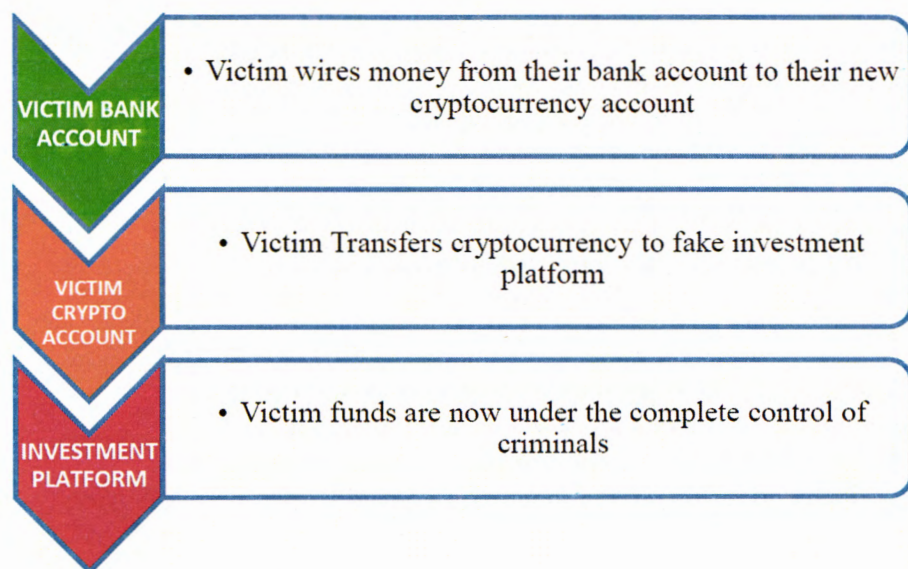
30. The fraud scheme detailed below is a particular type of investment fraud scheme known by an unsavory term - not repeated here - derived from the foreign-language word used to describe the scheme.

31. Based on data submitted to the FBI's Internet Crime Complaint Center in 2024, the particular type of investment fraud scheme detailed below targeted tens of thousands of victims in the United States and resulted in over \$5.8 billion in private assets being siphoned

overseas. The scheme begins with fraudsters contacting potential victims through seemingly misdirected text messages, dating applications, or professional meet-up groups. Next, using various means of manipulation, the fraudster gains the victim's affection and trust.

32. Once trust is established, the fraudster recommends cryptocurrency investment by touting their own success, or that of an associate. Means of carrying out the scheme vary, but a common tactic is to direct a victim to a fake "investment platform" hosted on a website.

33. These websites, and the "investment platforms" hosted there, are created by fraudsters to appear to be legitimate platforms. The fraudster assists the victim with opening a cryptocurrency account, often on a U.S.-based virtual currency exchange (VCE) such as Kraken or Crypto.com, and then walks the victim through transferring money from a bank account to that cryptocurrency account. Next, the victim will receive instructions on how to transfer their cryptocurrency assets to the fake investment platform. On its surface, the platform shows lucrative returns, encouraging further investment; underneath, all transferred funds are routed to a cryptocurrency wallet address controlled completely by the fraudsters.



34. Perpetrators of the particular type of investment fraud scheme detailed below frequently allow victims to withdraw some of their “profits” early in the scheme to engender trust and help convince victims of the legitimacy of the platform. As the scheme continues, victims are unable to withdraw their funds and are provided various excuses as to why. For example, the fraudsters will often refer to a fake “tax” requirement, stating that taxes must be paid on the proceeds generated from the platform. This is just an eleventh-hour effort by the fraudsters to elicit more money from victims. Ultimately, victims are locked out of their account and lose all their funds.

35. First employed by Chinese organized crime groups, the particular type of investment fraud scheme detailed below initially targeted victims inside China then expanded worldwide during the global pandemic. Operating from compounds in Cambodia and Myanmar, these criminal syndicates often operate by forcing human trafficking victims in Southeast Asia to participate in the schemes against their will. The schemes take advantage of the ability of cryptocurrency to be transferred securely and globally, without intermediaries and the safeguards established, and inherent to, the traditional financial system.

VI. *N.D. OHIO VICTIM.*

36. On or about September 3, 2024, a victim in Solon, Ohio, with the initials “S.W.” filed a complaint with the FBI’s Internet Crime Complaint Center. The fraud began when S.W. was contacted on July 22, 2024, by a woman on LinkedIn going by the name of Kristina Tian, who claimed to have a degree from Stanford and work at Mucker Capital. S.W. began exchanging information about investing with his new “friend” (hereinafter, “SUBJECT-1”). SUBJECT-1 suggested that they move their conversation to the messaging platform WhatsApp.

After building a relationship and establishing herself to S.W. as a successful investor, SUBJECT-1 suggested S.W. invest in cryptocurrencies at her direction.

37. During their correspondence, S.W. showed SUBJECT-1 screenshots of a portion of his investment holdings to prove to her that he had money to invest. S.W. already had a cryptocurrency account at Kraken (a VCE) before interacting with SUBJECT-1. In total, S.W. converted approximately \$500,000.00 of his money and wired it to his VCE account at Kraken. SUBJECT-1 then instructed S.W. what (fake) investment platform to use for the investments and where to transfer his Kraken cryptocurrency.

38. Before making his larger investments, S.W. tested the (fake) investment platform's legitimacy by requesting a return of a portion of funds from his first investment. After the request was processed successfully and funds were returned to S.W., S.W. was convinced that the investment platform was legitimate and continued with additional investments.

39. After seeing the alleged success of his initial investments, S.W. planned to invest a total of \$1.5 million in the cryptocurrency investments suggested by SUBJECT-1. On July 30, 2024, FBI personnel contacted S.W. and advised him that through an ongoing investigation he was identified as a potential victim of an investment fraud scheme. S.W. was set to make an additional \$200,000.00 investment the next day, which he ultimately did not do after speaking with the FBI.

40. After learning that he had been the victim of a scam, S.W. confronted SUBJECT-1 via WhatsApp. SUBJECT-1 responded with the following series of (mocking) messages over the course of 10 minutes:

MESSAGE 1 - 4:11 p.m.: **I feel for you.**

MESSAGE 2 - 4:12 p.m.: **You're a good pig, just not fat enough.**

MESSAGE 3 - 4:13 p.m.: **But thank you for giving me half of your savings.**

MESSAGE 4 - 4:20 p.m.: **Lol, I enjoyed it, and thank you for the money so I can find more.**

MESSAGE 5 - 4:20 p.m.: 🙄

MESSAGE 6 - 4:20 p.m.: **Glad to use your life savings.**

VII. *ARIZONA VICTIM.*

41. "J.C.", a resident of Arizona, met a man (hereinafter, "SUBJECT-2") on the dating app Coffee Meets Bagel. After spending time exchanging messages and building a relationship, SUBJECT-2 suggested that J.C. invest in cryptocurrencies.

42. J.C. used an account at Crypto.com to make the initial purchase of cryptocurrency to invest.

43. In or about July 2024, J.C. transferred the purchased cryptocurrency to the cryptocurrency address that SUBJECT-2 recommended, which J.C. believed to be the investment platform that SUBJECT-2 recommended. Later, J.C. was unable to retrieve the funds she "invested."

44. J.C. lost approximately \$63,000.00 from the investment fraud scheme in which she was directed by SUBJECT-2. This included a \$15,000.00 cashout of her 401(k) account for the "investment" and a HELOC loan for \$48,000.00 that J.C.'s daughter took out and provided to J.C. to invest.

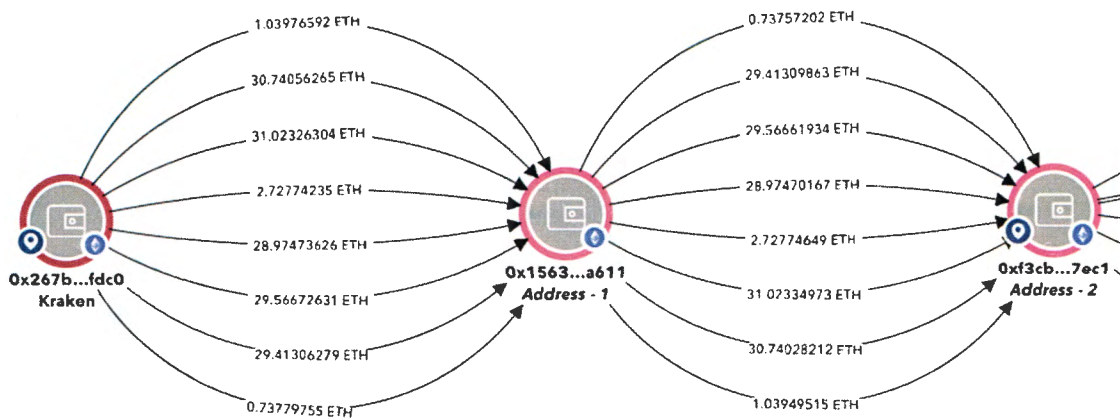
VIII. *TRACING ANALYSIS: FORFEITURE OF ALL TETHER ("USDT") CRYPTOCURRENCY (NAMELY, 501,595.10 USDT VALUED AT \$501,595.10) HELD AT ADDRESS-12.*

45. From July 24, 2024 through July 30, 2024, S.W. made at least eight transfers of ETH from his account at Kraken - totaling approximately \$495,079.00 - to the (fake) investment

platform - *i.e.*, cryptocurrency address beginning/ending 0x156 . . . 8a8a611 (ADDRESS-1) - which S.W. believed to be a Coinbase wallet address:

- July 24 - 1.03976592 ETH (\$3,607)
- July 25 - 30.74056265 ETH (\$95,683)
- July 25 - 31.02326304 ETH (\$96,563)
- July 26 - 2.72774235 ETH (\$8,915)
- July 29 - 28.97473626 ETH (\$94,830)
- July 29 - 29.56672631 ETH (\$96,767)
- July 29 - 29.41306279 ETH (\$96,265)
- July 30 - 0.73779755 ETH (\$2,449).

46. For each separate transfer into ADDRESS-1, the ETH was then transferred - on the same day of receipt - to the unhosted cryptocurrency address beginning/ending 0xf3c . . . c617ec1 (ADDRESS-2), as depicted below:



47. When the funds were received at ADDRESS-2, the theft of S.W.'s funds was complete. The funds were under the custody and control of the fraudsters.

48. After the transfers of the approximately \$495,079.00 of S.W.'s funds into ADDRESS-2, they were then swapped from ETH to DAI. Following the swaps, the resulting DAI was combined with other funds, which also appear to be funds related to investment fraud schemes. The following transfers then occurred:

a.) On July 25, 2024, a transfer of 105,892 DAI (\$105,892) - which included \$99,459 of S.W.'s funds - was made to cryptocurrency address beginning/ending 0x331 . . . c77f5db (ADDRESS-3).

b.) On July 29, 2024, a transfer of 98,193 DAI (\$98,193) - which included \$97,356 of S.W.'s funds - was made to ADDRESS-3.

c.) On July 25, 2024, a transfer of 98,576 DAI (\$98,576) - which included \$97,536 of S.W.'s funds - was made to cryptocurrency address beginning/ending 0x080 . . . 2e2e72c (ADDRESS-4).

d.) On July 27, 2024, a transfer of 9,751 DAI (\$9,751) - which included \$8,742 of S.W.'s funds - was made to ADDRESS-4.

e.) On July 29, 2024, a transfer of 97,628 DAI (\$97,628) - which included \$97,628 of S.W.'s funds - was made to ADDRESS-4.

f.) On July 30, 2024, a transfer of 98,040 DAI (\$98,040) - which included \$97,002 of S.W.'s funds - was made to ADDRESS-4.

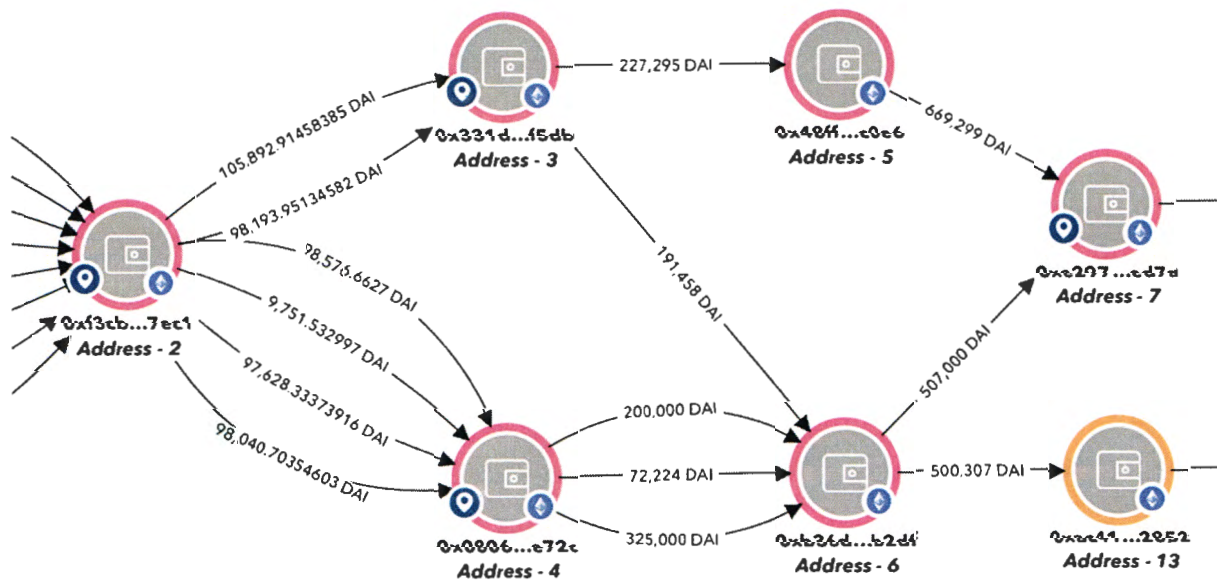
49. After S.W.'s funds ended up in ADDRESS-3 and ADDRESS-4, they were subsequently transferred - with other funds - to either the cryptocurrency address beginning/ending 0x48f . . . 92dc0e6 (ADDRESS-5) or the cryptocurrency address beginning/ending 0xb36 . . . 59ab2df (ADDRESS-6) between July 25, 2024 and July 30, 2024.

50. Using the Proceeds In, First Out tracing methodology, ADDRESS-5 contained 99,459 DAI (\$99,459) of S.W.'s funds.

51. Using the Proceeds In, First Out tracing methodology, ADDRESS-6 contained 398,246 DAI (\$398,246) of S.W.'s funds.

52. From ADDRESS-5 and ADDRESS-6, 196,995 DAI (\$196,995) of funds belonging to S.W. ended up at the cryptocurrency address beginning/ending 0xe29 . . . 9f3ed7a (ADDRESS-7) as part of transfers of 669,299 DAI and 507,000 DAI made on July 26, 2024.

53. From ADDRESS-6, 291,986 DAI (\$291,986) of funds belonging to S.W. ended up at the cryptocurrency address beginning/ending 0xac4 . . . 5c92852 (ADDRESS-13) by a transfer of 500,307 DAI made on July 30, 2024:



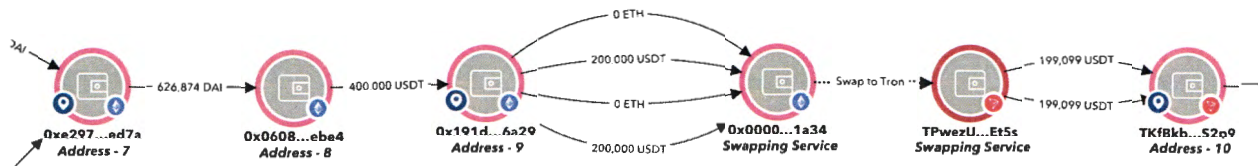
54. As stated, of the DAI transferred into ADDRESS-7, 196,995 DAI (\$196,995) were funds belonging to S.W. Thereafter, all on September 6, 2024, the following transfers occurred:

a.) From ADDRESS-7, 626,874 DAI - which included the 196,995 DAI (\$196,995) of S.W.'s funds - was transferred on September 6, 2024, to the cryptocurrency address

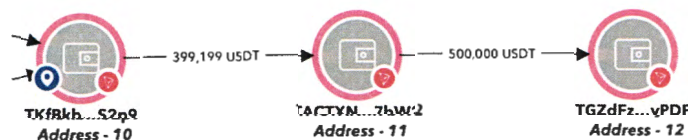
beginning/ending 0x060 . . . 81febe4 (ADDRESS-8), where it was swapped for Tether (“USDT”) cryptocurrency.

b.) Within five minutes of the swap, 400,000 USDT - of which 196,995 USDT (\$196,995) belonged to S.W. - was transferred to the cryptocurrency address beginning/ending 0x191 . . . a196a29 (ADDRESS-9).

c.) From ADDRESS-9, 400,000 USDT - of which 196,995 USDT (\$196,995) belonged to S.W. - was then transferred on September 6, 2024, to an address controlled by a swapping service, where the USDT on the Ethereum blockchain was swapped for a total of 398,198 USDT on the Tron blockchain. The resulting USDT on the Tron blockchain - of which 196,995 USDT (\$196,995) belonged to S.W. - was transferred on September 6, 2024, to the cryptocurrency address beginning/ending TKfBk . . . zWxS2p9 (ADDRESS-10), as depicted:



d.) Still on September 6, 2024: Within one hour of the USDT arriving in ADDRESS-10, the funds - of which 196,995 USDT (\$196,995) belonged to S.W. - were then moved to the cryptocurrency address beginning/ending TACTX . . . PWd7bW2 (ADDRESS-11). Within five minutes of that transfer, a total of 500,000 USDT - which included the USDT belonging to S.W. - was moved to the subject cryptocurrency address beginning/ending TGZdF . . . mYHyPDF (ADDRESS-12).



55. As set forth above, J.C. (the Arizona victim) lost approximately \$63,000.00 in the investment fraud scheme. Approximately 46,252 USDT (\$46,252) of J.C.'s funds ended up in the subject cryptocurrency address beginning/ending TGZdF . . . mYHyPDF (**ADDRESS-12**). Particularly, this 46,252 USDT was included with the 196,995 USDT belonging to S.W. in the September 6, 2024, transfer of the 500,000 USDT into **ADDRESS-12**.

56. On September 8, 2024, the USDT in **ADDRESS-12** was frozen by Tether Limited. At the time of the freeze, **ADDRESS-12** had a balance of approximately 501,595.10 USDT (\$501,595.10); *i.e.*, the 500,000 USDT transferred into the address on September 6, 2024 and a pre-existing balance of 1,595.10 USDT.

IX. *TRACING ANALYSIS: FORFEITURE OF ALL TETHER ("USDT") CRYPTOCURRENCY (NAMELY, 178,386.12 USDT VALUED AT \$178,386.12) HELD AT ADDRESS-17.*

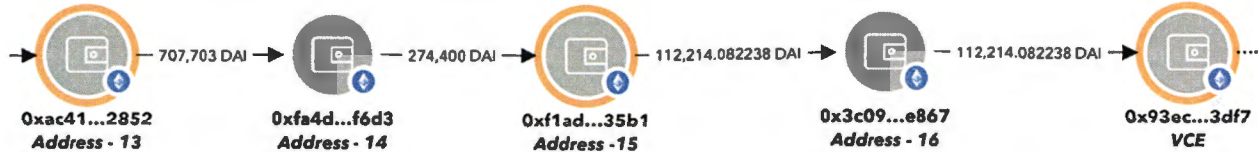
57. As set forth in paragraph 53 herein, using the Proceeds In First Out tracing methodology, 291,986 DAI (\$291,986) of funds belonging to S.W. ended up at the cryptocurrency address beginning/ending 0xac4 . . . 5c92852 (**ADDRESS-13**) as part of the transfer of 500,307 DAI made from **ADDRESS-6** on July 30, 2024.

58. From **ADDRESS-13**, 707,703 DAI - of which 291,986 DAI (\$291,986) belonged to S.W. - was transferred on September 27, 2024, to the cryptocurrency address beginning/ending 0xfa4 . . . 7c8f6d3 (**ADDRESS-14**).

59. On September 28, 2024, 274,400 DAI (\$274,400) - all belonging to S.W. - was transferred to the cryptocurrency address beginning/ending 0xf1a . . . 07635b1 (**ADDRESS-15**).

60. On September 30, 2024, 112,214 DAI (\$112,214) - all belonging to S.W. - was transferred from **ADDRESS-15** to the cryptocurrency address beginning/ending 0x3c0 . . . 959e867 (**ADDRESS-16**).

61. On October 4, 2024, the 112,214 DAI (\$112,214) - all belonging to S.W. - was transferred to an account at Binance, as depicted below:



62. Within the account at Binance, the 112,214 DAI (\$112,214) - all belonging to S.W. - was involved in trades that resulted in 112,214 USDT (\$112,214) on the Tron network. On October 13, 2024, a total of 178,386.12 USDT - which included the 112,214 USDT belonging to S.W. - was transferred to the subject cryptocurrency address beginning/ending THr7k . . . q9gskdN (ADDRESS-17).



63. On October 16, 2024, the USDT in ADDRESS-17 was frozen by Tether Limited. At the time of the freeze, ADDRESS-17 had a balance of approximately 178,386.12 USDT (\$178,386.12); *i.e.*, the 178,386.12 USDT transferred into the address on October 13, 2024.

X. *CONCLUSION: FORFEITURE OF ALL TETHER ("USDT") CRYPTOCURRENCY (NAMELY, 501,595.10 USDT VALUED AT \$501,595.10) HELD AT ADDRESS-12.*

64. Based upon the foregoing, the defendant 501,595.10 USDT (\$501,595.10) constitutes, or is derived from, proceeds traceable to wire fraud/wire fraud conspiracy and, further, was involved in a transaction in violation of 18 U.S.C. § 1957 (transactional money laundering) and/or 18 U.S.C. § 1956(a)(1)(B)(i) (concealment money laundering), or is property traceable to such property.

65. The transfer of the 500,000 USDT on September 6, 2024, from ADDRESS-11 to **ADDRESS-12** constituted a monetary transaction in violation of 18 U.S.C. § 1957 (transactional money laundering). Under 18 U.S.C. § 981(a)(1)(A), all property - real and personal - “involved in” or traceable to an offense in violation of § 1957 is subject to forfeiture. As set forth in paragraphs 54(d) and 55, the transfer of the 500,000 USDT to **ADDRESS-12** on September 6, 2024, included the 196,995 USDT belonging to S.W., the 46,252 USDT belonging to J.C., and other funds. Under § 1957, the entire 500,000 USDT is forfeitable as the corpus of the money laundering offense.

66. The transfer of the 500,000 USDT on September 6, 2024, from ADDRESS-11 to **ADDRESS-12** also constituted a transaction in violation of 18 U.S.C. § 1956(a)(1)(B)(i) (concealment money laundering). At the time of the transfer, **ADDRESS-12** had a pre-existing balance of approximately 1,595.10 USDT.

67. Under 18 U.S.C. § 981(a)(1)(A), all property - real and personal - “involved in” or traceable to an offense in violation of § 1956(a)(1)(B)(i) is subject to forfeiture. Particularly, “other funds” in a cryptocurrency address into which SUA proceeds are transferred as part of a concealment money laundering offense - along with any “other funds” transferred with the SUA proceeds as part of the concealment money laundering offense - are subject to forfeiture as property “involved in” the offense. In both instances, the “other funds” commingled with the SUA proceeds obfuscate the origin or existence of the SUA proceeds.

68. Under 18 U.S.C. § 981(a)(1)(A), the entire defendant property - namely, the 501,595.10 USDT (\$501,595.10) - is forfeitable. Both the “other funds” that were commingled with the SUA proceeds (*i.e.*, the SUA proceeds consisted of the 196,995 USDT belonging to S.W. and the 46,252 USDT belonging to J.C.) in the September 6, 2024, transfer of the 500,000

USDT from ADDRESS-11 to **ADDRESS-12** and the pre-existing balance of approximately 1,595.10 USDT in **ADDRESS-12** were “involved in” the concealment money laundering offense and, accordingly, are subject to forfeiture in that they facilitated the violation by helping to conceal the nature, source, ownership, and/or control of the USDT traceable to S.W. and J.C.

69. The entire defendant property - namely, 501,595.10 USDT (\$501,595.10) - also is subject to forfeiture under 18 U.S.C. § 981(a)(1)(C) as property which constitutes, or is derived from, proceeds traceable to an offense(s) constituting “specified unlawful activity” - as defined in 18 U.S.C. § 1956(c)(7), with reference to 18 U.S.C. § 1961(l) - namely: wire fraud, in violation of 18 U.S.C. § 1343, and wire fraud conspiracy, in violation of 18 U.S.C. § 371. In addition to the funds stolen from S.W. and J.C., the other USDT funds seized from **ADDRESS-12** appear to be the proceeds of fraud in that they bear indicia of the particular type of investment fraud scheme detailed above.

XI. *CONCLUSION: FORFEITURE OF ALL TETHER (“USDT”) CRYPTOCURRENCY (NAMELY, 178,386.12 USDT VALUED AT \$178,386.12) HELD AT **ADDRESS-17**.*

70. Based upon the foregoing, the defendant 178,386.12 USDT (\$178,386.12) constitutes, or is derived from, proceeds traceable to wire fraud/wire fraud conspiracy and, further, was involved in a transaction in violation of 18 U.S.C. § 1957 (transactional money laundering) and/or 18 U.S.C. § 1956(a)(1)(B)(i) (concealment money laundering), or is property traceable to such property.

71. The transfer of the 178,386.12 USDT on October 13, 2024, from the account at Binance to **ADDRESS-17** constituted a monetary transaction in violation of 18 U.S.C. § 1957 (transactional money laundering). Under 18 U.S.C. § 981(a)(1)(A), all property - real and personal - “involved in” or traceable to an offense in violation of § 1957 is subject to forfeiture. As set forth in paragraph 62, the transfer of the 178,386.12 USDT into **ADDRESS-17** on

October 13, 2024, included the 112,214 USDT belonging to S.W. and other funds. Under Section 1957, the entire 178,386.12 USDT is forfeitable as the corpus of the money laundering offense.

72. The transfer of the 178,386.12 USDT on October 13, 2024, from the account at Binance to **ADDRESS-17** also constituted a transaction in violation of 18 U.S.C. Section 1956(a)(1)(B)(i) (concealment money laundering). At the time of the transfer, **ADDRESS-17** had a pre-existing balance of 00.00.

73. Under 18 U.S.C. § 981(a)(1)(A), all property - real and personal - “involved in” or traceable to an offense in violation of § 1956(a)(1)(B)(i) is subject to forfeiture. Particularly, “other funds” transferred with the SUA proceeds as part of the concealment money laundering offense are subject to forfeiture as property “involved in” the offense. In that instance, the “other funds” commingled with the SUA proceeds obfuscate the origin or existence of the SUA proceeds.

74. Under 18 U.S.C. § 981(a)(1)(A), the entire defendant property - namely, 178,386.12 USDT (\$178,386.12) - is forfeitable. The “other funds” that were commingled with the SUA proceeds - *i.e.*, the SUA proceeds consisted of the 112,214 USDT belonging to S.W. - in the October 13, 2024, transfer of the 178,386.12 USDT from the account at Binance to **ADDRESS-17** were “involved in” the concealment money laundering offense and, accordingly, are subject to forfeiture in that they facilitated the violation by helping to conceal the nature, source, ownership, and/or control of the USDT traceable to S.W.

75. The entire defendant property - namely, 178,386.12 USDT (\$178,386.12) - also is subject to forfeiture under 18 U.S.C. § 981(a)(1)(C) as property which constitutes, or is derived from, proceeds traceable to an offense(s) constituting “specified unlawful activity” - as defined

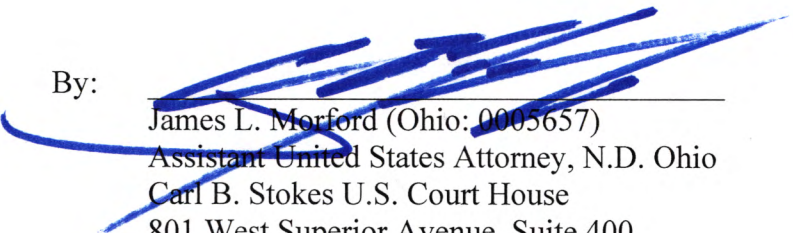
in 18 U.S.C. § 1956(c)(7), with reference to 18 U.S.C. § 1961(l) - namely: wire fraud, in violation of 18 U.S.C. § 1343, and wire fraud conspiracy, in violation of 18 U.S.C. § 371. In addition to the funds stolen from S.W., the other USDT funds seized from **ADDRESS-17** appear to be the proceeds of fraud in that they bear indicia of the particular type of investment fraud scheme detailed above.

WHEREFORE, plaintiff, the United States of America, requests that the Court enter judgment condemning the defendant properties and forfeiting them to the United States, and providing that the defendant properties be delivered into the custody of the United States for disposition in accordance with law and for such other relief as this Court may deem proper.

Respectfully submitted,

Carol M. Skutnik
Acting United States Attorney, N.D. Ohio

By:

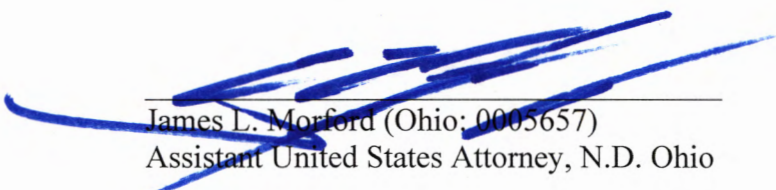


James L. Morford (Ohio: 0005657)
Assistant United States Attorney, N.D. Ohio
Carl B. Stokes U.S. Court House
801 West Superior Avenue, Suite 400
Cleveland, Ohio 44113
216.622.3743 / James.Morford@usdoj.gov

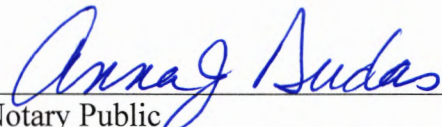
VERIFICATION

STATE OF OHIO)
) SS.
COUNTY OF CUYAHOGA)

I, James L. Morford, under penalty of perjury, depose and say that I am an Assistant United States Attorney for the Northern District of Ohio, and the attorney for the plaintiff in the within entitled action. The foregoing Complaint in Forfeiture is based upon information officially provided to me and, to my knowledge and belief, is true and correct.


James L. Morford (Ohio: 0005657)
Assistant United States Attorney, N.D. Ohio

Sworn to and subscribed in my presence this 29th day of May, 2025.


Notary Public



ANNA J DUDAS
Notary Public
State of Ohio
My Comm. Expires
December 5, 2026