

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

ALEXANDRIA DIVISION

IN THE MATTER OF THE SEIZURE OF ALL
USDT TOKENS HELD IN A CRYPTOCURRENCY
WALLET ADDRESS IDENTIFIED BY
0x9AFc36B20C961CD34450ae0C3941C302bfd6B1F1

Case No. 1:24-sw-603

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEIZURE WARRANT

I, Yanira Nieves, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a “federal law enforcement officer” within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(c), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a seizure warrant.

2. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and have been so employed since about April 2023. I am assigned to one of the Washington Field Office’s White-Collar Crime Squads where I investigate violations of federal laws including wire fraud, cryptocurrency crimes, securities fraud, and commodities fraud. I have completed about 20 weeks of New Agent Training in legal statutes, procedures, and investigations at the FBI Academy at Quantico. I have received specialized training in cryptocurrency investigations and digital investigative techniques. From in and around 2015 to 2022, I was an FBI Intelligence Analyst where I worked on cyber and criminal investigations that involved wire fraud, securities fraud, and commodities fraud. In addition, I have a bachelor’s degree in Business Administration from the University of Puerto Rico, Bayamon, where I majored in Accounting and Finance, and a Master of Business Administration from the University of Puerto Rico, Rio Piedras. I am also a Certified Public Accountant licensed in Puerto Rico. I have not included every detail of my

training, education, and experience, but have highlighted those areas most relevant to this application. I am an “investigative or law enforcement officer” of the United States within the meaning of 18 U.S.C. § 2510(7), in that I am empowered by law to conduct investigations and to make arrests for federal felony offenses.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of 18 U.S.C. § 1343 (Wire Fraud); 18 U.S.C. § 1956(h) (Conspiracy to Commit Money Laundering) and 18 U.S.C. § 1957 (Engaging in Monetary Transactions in Property Derived from Specific Unlawful Activity), have been committed by unidentified parties. There is also probable cause to seize the **TARGET PROPERTY** described in Attachment A as property subject to forfeiture pursuant to 18 U.S.C. §§ 982(a)(1) and 981(a)(1)(A).

PROPERTY TO BE SEIZED

4. The affidavit is made to obtain a seizure warrant for **all USDT tokens** (“**TARGET PROPERTY**”) held in virtual cryptocurrency wallet address identified by x9AFc36B20C961CD34450ae0C3941C302bfd6B1F1 (“**TARGET ADDRESS**”).

APPLICABLE LAW

5. 18 U.S.C. § 1343 (Wire Fraud) 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, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be guilty of a federal offense.

6. 18 U.S.C. § 1956(a)(1)(B)(i) (concealment money laundering) prohibits, in pertinent part, 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 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.

7. 18 U.S.C. § 1957 (unlawful monetary transaction) prohibits, where the offense takes place in the United States, knowingly engaging or attempting to engage in a monetary transaction in criminally derived property of a value greater than \$10,000 and derived from specified unlawful activity.

8. 18 U.S.C. § 981(a)(1)(C) (forfeiture for specified unlawful activities) provides for the forfeiture of any property, real or personal, which constitutes or is derived from proceeds traceable to any offense constituting a specified unlawful activity (“SUA”), as defined in 18 U.S.C. § 1956(c)(7), or a conspiracy to commit such SUA. 18 U.S.C. § 1956(c)(7)(A) provides that any act or activity constituting an offense under 18 U.S.C. § 1961(1) constitutes an SUA, with the exception of an act indictable under subchapter II of Chapter 53 of Title 31 of the U.S. Code. 18 U.S.C. § 1961(1) references violations of 18 U.S.C. § 1343.

9. 28 U.S.C. § 2461(c) (civil to criminal forfeiture incorporation statute) provides that if a person is charged in a criminal case with a violation for which the civil or criminal forfeiture of property is authorized, the government may include notice of the forfeiture in the

charging instrument pursuant to the Rules of Criminal Procedure. If the defendant is convicted of the offense giving rise to forfeiture, the Court shall order forfeiture of the property as part of the defendant's sentence. The procedures of 21 U.S.C. § 853 shall apply to all stages of a criminal forfeiture proceeding, except for subsection (d) of that statute.

10. Pursuant to 18 U.S.C. §§ 982(a)(1) and 981(a)(1)(A), any property, real or personal, which was involved in a violation of 18 U.S.C. § 1956 and 18 U.S.C. § 1957 (Engaging in Monetary Transactions in Property Derived from Specified Unlawful Activity), is subject to criminal and civil forfeiture. Moreover, any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of those same two offenses is subject to forfeiture pursuant to 18 U.S.C. § 982(a)(1), 18 U.S.C. § 981(a)(1)(A), and 28 U.S.C. § 2461(c).

11. Section 981(b)(3) (civil seizures) provides that, “[n]otwithstanding the provisions of rule 41(a) of the Federal Rules of Criminal Procedure, a seizure warrant may be issued pursuant to this subsection by a judicial officer in any district in which a forfeiture action against the property may be filed under [28 U.S.C. § 1355(b)] and may be executed in any district in which the property is found, or transmitted to the central authority of any foreign state for service in accordance with any treaty or other international agreement.” 18 U.S.C. § 981(b)(3). Pursuant to 28 U.S.C. § 1355(b), a forfeiture action may be brought in any district court where any of the acts giving rise to the forfeiture occurred, even as to property located outside the district.

12. 21 U.S.C. § 853(f) (criminal seizures) provides that the government may request a seizure warrant authorizing the seizure of property subject to forfeiture in the same manner as for a search warrant. The seizure warrant issues if the Court determines that there is probable cause to believe that the property seized would, in the event of conviction, be subject to forfeiture and

that a restraining order may not be sufficient to assure the availability of such property for forfeiture.

13. A restraining order would be inadequate to preserve the cryptocurrency for forfeiture. Based on my training and experience, I know that restraining orders served on banks sometimes fail to preserve the property for forfeiture because the bank representative receiving the restraining order fails to put the necessary safeguards in place to freeze the money in time to prevent the account holder from accessing the funds electronically or fails to notify the proper personnel as to the existence of the order. The risk of such problems is higher, not lower, with virtual currency. In contrast, a seizure warrant guarantees that the funds will be in the government's custody upon execution of the warrant and, thus, preserved for forfeiture. The USDT is currently temporarily frozen. Given that the TARGET ADDRESS frequently moves cryptocurrency and swaps cryptocurrency, there is a concern that if the **TARGET PROPERTY** is not quickly seized or otherwise restrained the USDT may no longer be in the account.

14. One of the chief goals of forfeiture is to remove the profit from crime by separating the criminal from his or her dishonest gains, and to divest criminal actors from the apparatus allowing them to engage in criminal activity. *See Kaley v. United States*, 571 U.S. 320, 323 (2014). To that end, in cases involving a money laundering offense, the forfeiture statutes connected to money laundering offenses permit the government to forfeit property "involved in" money laundering. Such property includes "untainted property" commingled with "tainted" property, when that untainted property is used to facilitate the laundering offense, such as by obscuring the nature, source, location, or control of any criminally derived property. *See* Title 18, United States Code, Sections 981(a)(1)(A), 982(a)(1); *see also United States v. Miller*, 911 F.3d 229, 234 (4th Cir. 2018); *United States v. Kivanc*, 714 F.3d 782, 794-95 (4th Cir. 2013).

PROBABLE CAUSE

I. BACKGROUND REGARDING VIRTUAL CURRENCY

15. **Virtual Currency:** 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 rather are generated and controlled through computer software. Bitcoin is currently one of the most popular virtual currencies in use.

16. **Virtual Currency Address:** Virtual currency addresses are the digital 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. Based on my training and experience, I know that it is possible to “swap”, or otherwise, exchange cryptocurrencies by using Decentralized Exchanges (DEX’s). DEX’s allow for the swapping of one cryptocurrency for another by keeping large liquidity pools of various cryptocurrency types, which users can then swap between for a nominal fee. Unlike Centralized Cryptocurrency Exchanges, DEX’s are not custodial, and allow for these swaps through the use of smart contracts, and therefore avoid the need for a third party to ever have custody of the cryptocurrencies being swapped.

17. **Virtual Currency Exchange:** Virtual currency exchanges, such as Crypto.com are trading and/or storage platforms for virtual currencies. Many exchanges also store their customers’ virtual currency in virtual currency accounts. These virtual currency accounts are commonly referred to as wallets and can hold multiple virtual currency addresses.

18. **Blockchain:** Many virtual currencies, including Ether, publicly record all their transactions on what is known as a blockchain. The blockchain is a distributed public ledger containing an immutable and historical record of every transaction utilizing that blockchain’s

technology. The blockchain can be updated multiple times per hour and records every virtual currency address that has ever received that virtual currency and maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies. It should be noted that, due to the international nature of virtual currencies, most blockchain explorers operate using the Coordinated Universal Time (UTC) Zone. The times/dates used in this affidavit are also based on the UTC time zone.

19. **Blockchain Analysis:** While the identity of a virtual currency address owner is generally anonymous, law enforcement can identify the owner of a particular virtual currency address by analyzing the blockchain (e.g., the Ethereum blockchain). The analysis can also reveal additional addresses controlled by the same individual or entity. “For example, when an organization creates multiple Ethereum addresses, it will often combine its Ethereum addresses into a separate, central Bitcoin address (i.e., a “cluster”). It is possible to identify a ‘cluster’ of Ethereum addresses held by one organization by analyzing the Ethereum blockchain’s transaction history. Open source tools and private software products can be used to analyze a transaction.” *United States v. Gratkowski*, 964 F.3d 307, 309 (5th Cir. 2020).

20. **Company A:** Over the course of this investigation, the FBI conducted detailed blockchain analysis through “Company A” a company the FBI has a contracted with to do blockchain tracing and analytics. The company is located in the United States. Company A provides services to government agencies and private firms allowing for the tracking of cryptocurrency payments. Company A’s software helps track the public movements of cryptocurrency across the public blockchain ledger and private wallets.

21. **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 (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.

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

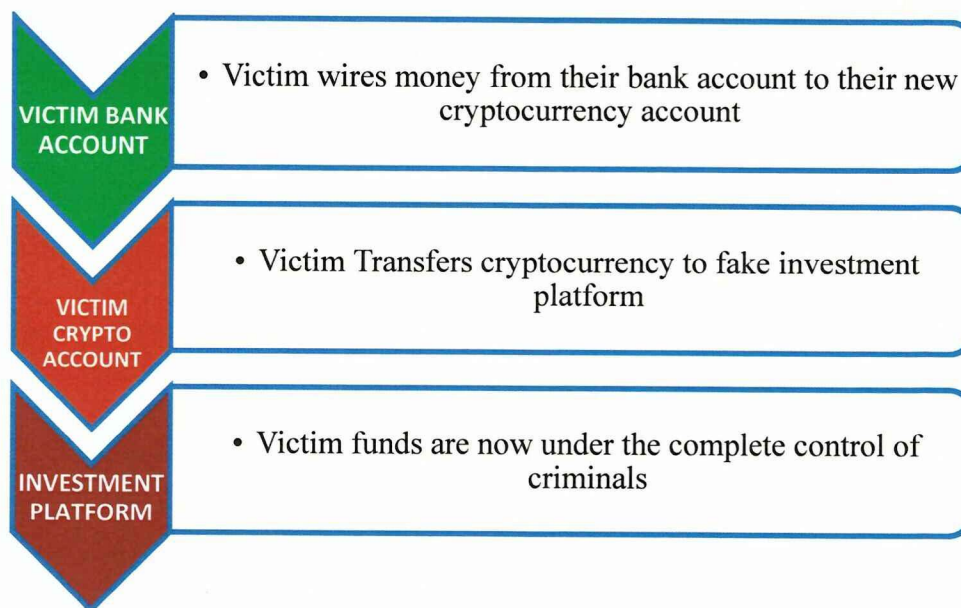
23. **Ether:** Ether ("ETH") is a cryptocurrency that is open-source and is distributed on a platform that uses "smart contract" technology. Transactions involving ETH are publicly recorded on the Ethereum blockchain, which allows anyone to track the movement of ETH.

24. **Bitcoin:** Bitcoin (or "BTC") is a type of virtual currency. Unlike traditional, government-controlled currencies (*i.e.*, fiat currencies), such as the U.S. dollar, Bitcoin is not managed or distributed by a centralized bank or entity. Because of that, Bitcoin can be traded without the need for intermediaries. Bitcoin transactions are approved/verified by computers running Bitcoin's software. Those computers are called network nodes. Each node uses cryptography to record every Bitcoin transaction on the Bitcoin blockchain. The Bitcoin blockchain is a public, distributed ledger. Bitcoin can be exchanged for fiat currency, other virtual currencies, products, and services.

25. **Cryptocurrency Investment Schemes ("Pig Butchering"):** The FBI is investigating an investment fraud scheme, referred to as "pig butchering," a term derived from the foreign-language word used to describe this scheme. Based on data submitted to the FBI's Internet Crime Complaint Center (located at <https://www.ic3.gov/>) in 2023 alone, cryptocurrency investment fraud, including pig butchering schemes, targeted tens of thousands of victims in the

United States and resulted in over 3.5 billion dollars in private assets being siphoned overseas. Pig butchering schemes begin by criminals contacting potential victims through seemingly misdirected text messages, dating applications, or professional meetup groups. Next, using various means of manipulation, the criminal gains the victim's affection and trust. Criminals refer to victims as "pigs" at this stage because they concoct elaborate stories to "fatten up" their victims.

26. Once that trust is established, the criminal recommends cryptocurrency investment by touting their own, or an associate's, success in the field. 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. These websites, and the investment platforms hosted there, are created by criminals to mimic legitimate platforms. The subject assists the victim with opening a cryptocurrency account, often on a U.S.-based exchange such as Coinbase, Crypto.com or Kraken, 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 deposited funds are routed to a cryptocurrency wallet address controlled completely by the criminals – the "butchering" phase of the scheme.



27. Pig butchering perpetrators 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 criminals will often levy a fake “tax” requirement, stating taxes must be paid on the proceeds generated from the platform. This is just an eleventh-hour effort by the criminals to elicit more money from victims. Ultimately, victims are locked out of their accounts and lose all their funds.

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

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

- **Layering** – Next, criminals will have victim funds transverse numerous private wallets, consolidate with other illegitimate and sometimes legitimate funds, and be subjected to other more cryptocurrency-specific processes to obfuscate both the origin of, and the ultimate destination for, the victim funds.
- **Integration** – Finally, by using a diffuse network of “brokers,” who agree to exchange cryptocurrency for fiat using various means, criminals render their proceeds liquid and fully integrated with the legitimate financial system.

II. PROBABLE CAUSE FOR SEIZURE OF TARGET PROPERTY

29. The victim, a resident of the Eastern District of Virginia, reported information to the FBI that establishes that the victim has been defrauded out of approximately \$86,158.00 between June 2024 and July 2024 in a Pig Butchering scheme.

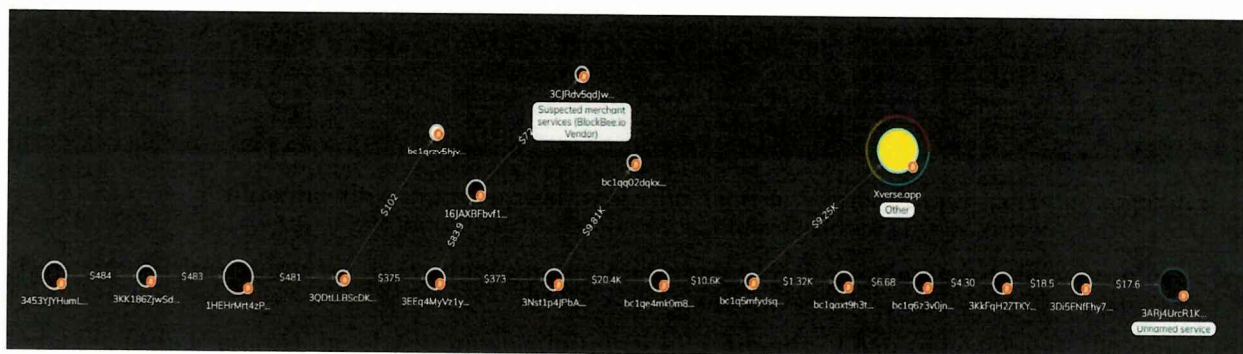
30. In June of 2024, the victim met the unknown subject(s), purportedly a man named David Andrésiak (DAVID) via Bumble, an online dating application. After matching on Bumble and speaking through Bumble’s chat function, DAVID suggested that they chat on Whatsapp. During their conversation via Whatsapp, DAVID claimed to be knowledgeable about short-term cryptocurrency trading, and eventually convinced the victim to begin investing with DAVID’s assistance.

31. DAVID walked the victim through setting up an account at Crypto.com, which is a Cryptocurrency exchange. DAVID explained that the victim could use the Crypto.com account to purchase cryptocurrency and then move that cryptocurrency into a Decentralized Finance (DeFi) wallet app.¹ Once in the Defi wallet app, the victim was informed they could

¹ DeFi wallet apps are virtual asset wallet applications in which users can participate in the finance sector without the use of traditional intermediaries such as brokerages, banks, or exchanges. Instead, the users can participate in investing, lending, borrowing, or other similar actions through peer-to-peer transactions, thus decentralizing the financial transactions from traditional intermediaries.

invest the cryptocurrency in a trading platform called Trustfuturesnum.com. The investigation revealed that Trustfuturesnum.com was created on or about February 2, 2024.

32. In June of 2024, at the direction of DAVID, the victim made an investment account at Trustfutures. On or about June 17, 2024, the victim sent \$500.00 from their CashApp account to their Crypto.com account. The victim then used their Crypto.com account to purchase 0.0073119 Bitcoin (BTC), valued at approximately \$483.00 USD. The victim then sent the 0.0073119 BTC to what the victim believed was their Trustfutures account. However, in actuality, the victim was sent the BTC to an unhosted BTC address, 1HEHrMrt4zPPFoggkUKYdnKSPADgCWMHW3, which is unrelated to any legitimate trading platform. This BTC was then sent by the subject(s) with control of this wallet to other wallets which eventually depleted the funds. A visual representation of the movement of the BTC is below:



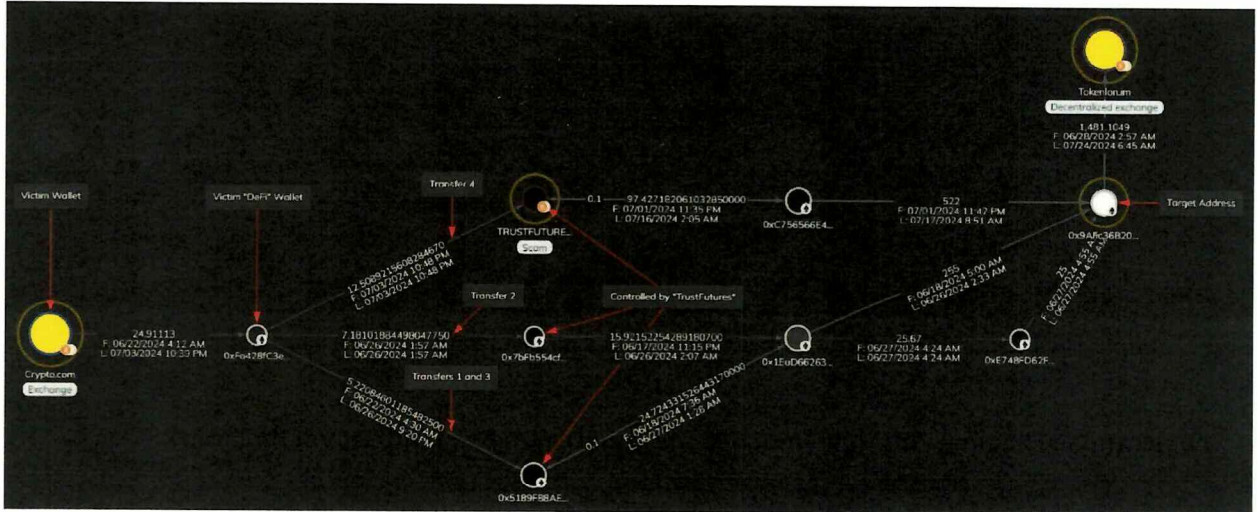
33. Following this initial investment, the victim’s Trustfutures account appeared to show significant returns on the victim’s initial investment. After seeing what the victim believed to be the initial returns, the victim made additional investments. Over the course of the following few weeks, the victim conducted four more investment transactions totaling \$83,436.16. Following these transactions, the victim believed they had made significant profit as their Trustfutures account showed a balance of \$322,803.99.

34. On or about July 9, 2024, the victim attempted to withdraw funds from their TrustFutures account. However, upon attempting to withdraw funds, DAVID became combative with the victim, and refused to approve the withdrawal. The victim used the chatbot function on TrustFutures to contact customer service about the withdrawal. TrustFutures Customer Service told the victim that in order to make a withdrawal the victim would first need to pay a 15% withdrawal fee, in the amount of approximately \$48,420.45. The victim was further told that if this fee was not paid within 7 business days, the funds might be lost in the blockchain.

35. The victim contacted DAVID again and requested that DAVID provide screenshots of his transactions from his TrustFutures account to prove that if an account holder pays the withdrawal fee, then the company will release the funds. DAVID provided the victim with some screenshots; however, the victim noticed several typos including the spelling of DAVID's name. The inability of the victim to make a withdrawal, the tactic of asking for additional fees, and the screenshots containing typos caused the victim to suspect that TrustFutures was an investment scam.

36. On or about July 15, 2024, the victim submitted a complaint to the FBI and was interviewed by your Affiant on or about July 18, 2024. Law enforcement traced each of the subsequent four transactions and the tracing shows that the cryptocurrency was not placed in the victim's investment account at TrustFutures, rather it was laundered through multiple Ethereum addresses before being deposited in the TARGET ADDRESS. The four transactions from the victim totaled approximately 24.9 Ethereum. Below is a visual representation of the movement of the four transactions, and the interconnectivity of many of these wallet addresses. It should be noted that the values of transferred ETH shown on the visual representation are the values of the

total amount of ETH transferred between two clusters between the dates that are listed. They do not necessarily represent single transfers of ETH.



37. Based on my training and experience, the movement of these funds is consistent with the methodology employed in many scams referred to using the umbrella term Pig-Butchering.

Transaction 1 – June 22, 2024, 04:12 UTC

38. On June 22, 2024, the victim transferred approximately 1.67253 ETH (valued at approximately \$5,861.70) from their Crypto.com account to their DeFi wallet, which the victim had also created with the assistance of DAVID. About 18 minutes later, the victim transferred approximately 1.67247 ETH from their DeFi wallet to 0x5189F88AEf4412120Db1Bad65329A55B4a08f2Fa (0x51), an address likely controlled by the individual(s) behind the scam.

39. About 7 minutes later approximately 1.67241 ETH was transferred from 0x51 to 0x1EaD66263c6559fc5868Ec7C2d7714CCcdCe4Bf9 (0x1EaD), where it was comingled with other funds. It remained in this address for about 5 days.

40. On June 27, 2024, 0x1EaD transferred approximately 25.67 ETH, including the victim funds, to 0xE748FD62F1671a1bc37A6e41FD16B1DcAA5Df357 (0xE7). About 31 minutes later, 0xE7 transferred approximately 25.00 ETH to the TARGET ADDRESS.

Transaction 2 – June 26, 2024, 01:43 UTC

41. On June 26, 2024, the victim transferred approximately 7.18109 ETH (valued at approximately \$24,328.88) from their Crypto.com account to their DeFi wallet. About 14 minutes later, the victim transferred approximately 7.18101 ETH from their DeFi wallet to 0x7bFb554cf05430FA19F1F75A0f03AAa535f811bb (0x7b), an address likely controlled by the individual(s) behind the scam.

42. About 10 minutes later approximately 7.18095 ETH was transferred from 0x7b to 0x1EaD, where it was comingled with other funds.

43. About 26 minutes later, 0x1EaD transferred approximately 28.00 ETH, including the victim funds, to the TARGET ADDRESS.

Transaction 3 – June 26, 2024, 21:12 UTC

44. About 19 hours and 29 minutes after the previous transaction conducted on June 26, 2024, the victim transferred approximately 3.5485 ETH (valued at approximately \$12,027.07) from their Crypto.com account to their DeFi wallet. About 8 minutes later, the victim transferred approximately 3.54837 ETH from their DeFi wallet to 0x5189F88AEf4412120Db1Bad65329A55B4a08f2Fa (0x51), an address likely controlled by the individual(s) behind the scam.

45. About 29 minutes later 3.5483 ETH was transferred from 0x51a to 0x1EaD, where it was comingled with other funds. It remained in this address for about 6 hours and 35 minutes.

46. On June 27, 2024, 0x1EaD transferred approximately 25.67 ETH, including the victim funds, to 0xE748FD62F1671a1bc37A6e41FD16B1DcAA5Df357 (0xE7). About 31 minutes later, 0xE7 transferred approximately 25.00 ETH to the TARGET ADDRESS.

Transaction 4 – July 3, 2024, 22:39 UTC

47. On July 3, 2024, the victim transferred approximately 12.50901 ETH (valued at approximately \$41,218.51) from their Crypto.com account to their DeFi wallet. About 14 minutes later, the victim transferred approximately 12.50892 ETH from their DeFi wallet to 0xd19632f884fE059C0Ed20f23912224015080C094 (0xd1), an address likely controlled by the individual(s) behind the scam. It should be noted that due to previous activity in this address, Company A's Software has already identified 0xd1 as being involved in a scam. As a result, it has been given the name of "TRUSTFUTURESCY.com" and the cluster bubble has been given a different appearance.

48. About 5 minutes later approximately 12.50892 ETH was transferred from 0xd1 to 0xC756566E4ad94764F1F00aBc4b650060Af99F891 (0xC756), where it was comingled with other funds.

49. The following day, on July 4, 2024, 0xd1 transferred approximately 35.00 ETH, including the victim funds, to the TARGET ADDRESS.

Activity of TARGET ADDRESS and Movement of Funds

50. The TARGET ADDRESS was created first on June 18, 2024, and continues to be active through at least August 2, 2024.

51. Over the course of this timespan, the TARGET ADDRESS has received approximately 1672.77 ETH, which is roughly equivalent to \$5,309,927.86 USD. Of that, at least 457.97 ETH of the ETH received by the TARGET ADDRESS has been received, either directly or indirectly, from other Ethereum addresses which are associated with previously identified investment scams. Of note, in addition to indirectly receiving funds from 0xd1, which is identified as being connected to “TRUSTFUTURESCY.com” (previously described above), the TARGET ADDRESS also receives indirect funding from other, similarly named scam clusters. Examples of such clusters are 0x2B99e2D6a4DA4F8231eBd566B571c4E71fb61eD5, identified as “TRUSTFUTURESBIT.com”, 0x2B99e2D6a4DA4F8231eBd566B571c4E71fb61eD5, identified as “TRUSTFUTURESOPT.com”, and other similar names, often including the words “Trust”, “DeFi”, and/or “Futures”. These names indicate, falsely, that they are related to futures trading and/or investing.

52. More specifically, two consolidation addresses previously mentioned, 0xC756 and 0x1EaD, receive a significant amount of ETH from clusters tied to other, similar Pig-Butchering schemes.

53. 0xC7 was active between July 1, 2024, and July 17, 2024. During this timeframe, it received approximately 545.63 ETH. Of this, approximately 325.9115 ETH came directly from 8 other clusters connected to related Pig-Butchering schemes. It should be noted that this only represents clusters that have already been identified as being connected to Pig-Butchering schemes, and does not mean that that the remaining ETH received by this address is sourced from legal sources.

54. 0x1EaD was active between June 17, 2024 and June 27, 2024. During this timeframe, it received approximately 285 ETH. Of this, approximately 41.86 ETH came directly from 4 other clusters connected to related Pig-Butchering schemes. As with 0xC756 above, this only represents clusters that have already been identified as being connected to Pig-Butchering schemes, and does not mean that that the remaining ETH received by this address is sourced from legal sources.

55. Furthermore, for both 0xC756 and 0x1EaD, their remaining funding originates almost exclusively from Crypto.com, and enters 0xC756 and 0x1EaD from intermediary wallets. Through my training and experience, I know that it is common for Pig-Butchering schemes to direct many of their victims to open accounts using the same Cryptocurrency Exchanges. In this particular scheme, the victim was directed to open an account using Crypto.com. It is therefore likely that many other victims were directed to do the same, thus explaining why the majority of the funds contained within 0xC756 and 0x1EaD originate from Crypto.com and then are transferred through various layers of scam addresses.

56. While the TARGET ADDRESS receives ETH directly and indirectly from multiple different sources, the TARGET ADDRESS sends ETH almost exclusively to one location, Tokenlon. Of the approximately 1,581.2149 ETH that the TARGET ADDRESS sends, approximately 1481.1049 ETH (about 93.66%) to Tokenlon. Tokenlon is a Decentralized Exchange (DEX). A DEX allows for the swapping of one virtual asset to another, while not requiring a third party to handle the transfer and does not collect Know Your Customer (KYC) information.

57. Based on my training and experience, I know that scammers involved in Pig-Butchering schemes will often use DEX's or similar swapping services to further their schemes.

Using a DEX and swapping one virtual asset for another further obfuscates the origin of the virtual assets and causes the tracing of such virtual assets to become more complex.

58. Furthermore, it is common to use DEX's to swap native tokens, such as Ether, to Stablecoins. Victims are commonly told to invest using virtual assets such as Bitcoin or Ether. While the victims are interested in investing with tokens that are subject to market changes, the scammers typically are not. To protect the value of the funds fraudulently obtained, scammers will often use DEX's or other swapping services to swap more volatile virtual assets to stable ones, particularly stablecoins pegged to the US Dollar, which as a fiat currency, is generally stable and strong in comparison to many other types of fiat foreign currencies.

59. Of the approximately 1672.77 ETH that the TARGET ADDRESS has received, the TARGET ADDRESS has sent approximately 1481.2149 ETH to Tokenlon, where the ETH was swapped for Tether (USDT) and returned to the TARGET ADDRESS.

60. Once swapped, the TARGET ADDRESS will then withdraw the USDT and send it to other addresses to continue the movement and laundering of the funds. The USDT is then eventually sent to Exchange accounts held in exchanges that are based overseas and outside the jurisdiction of the United States. Based on my training and experience, I know that a series of convoluted transactions and quick swaps from one type of cryptocurrency to another is a strong indication that the movement of funds was performed in a manner meant to conceal the nature, source, control, and/or ownership of the proceeds of a specified unlawful activity, to wit, wire fraud.

61. The TARGET ADDRESS is held in an unhosted wallet that has the capability of generating and using addresses that operate on the Ethereum Blockchain. This allows the

TARGET ADDRESS to send and receive both ETH and USDT by using the same Ethereum address.

62. Throughout this process, the TARGET ADDRESS has carried a large balance of ETH. Since the first transaction into the TARGET ADDRESS containing funds obtained fraudulently from the victim, the TARGET ADDRESS has never held less than 141.6552 ETH (valued at approximately \$425,904.77) at any given time. As the amount of ETH in the TARGET ADDRESS has never dropped below 24.9 between the day the victim's funds entered the TARGET ADDRESS and the date the TARGET ADDRESS was frozen, the victim's funds remain in the account as ETH.

63. As all the funds currently held in the TARGET ADDRESS are involved in money laundering, all of the funds—both ETH and USDT—are subject to forfeiture. While the victim transfers may have entered the TARGET ADDRESS as ETH, any USDT located within the TARGET ADDRESS constitutes property involved in money laundering as it helped conceal the nature, source, location, control, and/or ownership of the proceeds of a specified unlawful activity, to wit, wire fraud.

64. On August 2, 2024, the FBI sent a letter to Tether asking for a voluntary freeze of the **TARGET PROPERTY** in the TARGET ADDRESS. Tether informed the FBI that there is currently 300,000 USDT—\$300,000 U.S. dollar equivalent—in the TARGET ADDRESS.

65. The 300,000 USDT initially came from Sideshift.ai, an exchange and swapping service which is located in St. Kitts. From Sideshift, the funds are sent as ETH into two unhosted addresses, 0xA85975b9E69b589780A6a38b3A0128C5cE379d04 and 0xA525fa18D6b04538618B6a1AA8AC68c71eD262c0. Those addresses, in turn, sent the funds to a consolidation address, 0x6687F0e00B6C618e3A48045B253b08f5173684b7, which

swapped the ETH for USDT via Tokenlon. Following this, the funds were sent to 0x0D3B28EFF27670a3ADE8179cBB72F5efa63D672F (0x0D3), which then sent them to the TARGET ADDRESS, where they were frozen.

66. It should be noted that in addition to this 300,000 USDT specifically, between July 23, 2024 and July 30, 2024, 0x0D3 transferred an additional 680,000 USDT to the TARGET ADDRESS. 0x0D3, in total, sends approximately 980,000 USDT to the TARGET ADDRESS across four separate transactions within about seven days.

67. The pattern of movement for these funds is extremely similar to the movement of funds previously described regarding the specific transactions related to the victim as well as other cryptocurrency sent to the TARGET ADDRESS from other, related, scam addresses. Firstly, in all of these situations, ETH is transferred in an impractical manner through multiple unhosted wallets. This movement incurs an excessive amount of fees² which no normal investment group would pay. Secondly, in all of these situations, Tokenlon is used to swap ETH to USDT. As previously described, this is a very common methodology employed by scammers, particularly in Pig-Butchering cases. This allows scammers both to obfuscate and promote the laundering of these funds, while simultaneously protecting the value of their assets by moving away from a more volatile virtual asset such as ETH into a more stable one, such as USDT.

68. In total, the TARGET ADDRESS, over its lifespan, receives approximately 9,827,038.58 USDT. Of that, the majority of the USDT received by the TARGET ADDRESS, about 5,034,005.88 USDT (about 51.2%), is received as a result of the ETH to USDT swaps

² In order to conduct a transaction on the Ethereum Blockchain, a fee, sometimes referred to as gas, must be paid to fund the transfer. This fee is based on the current demand to conduct the transaction at the time of initiation, and can vary depending on demand, network traffic, and/or supply. The more transactions an individual conducts, the more fees are incurred. Thus, it is usually in the interest of the parties to reduce the number of transactions as much as possible to incur the least amount of fees.

conducted by the TARGET ADDRESS via Tokenlon. The second largest supplier of USDT to the TARGET ADDRESS is a different unhosted address, 0x86d63D835B0ff15D5719D4D155F2A169fE692a42 (0x86), which sends approximately 2,832,044.75 USDT to the TARGET ADDRESS, representing about 28.8% of the total USDT received by the TARGET ADDRESS.

69. This is notable because 0x86 is likely a separate consolidation wallet within the greater Pig-Butchering Scheme. Over its lifespan, 0x86 receives a total of approximately 2,9251,54.16 USDT. Of that, at least 923,432.95 USDT comes either directly or indirectly from other clusters identified associated with scams. These scams include, but are not limited to, NASDAWEB.com, NASDAQALL.com, and NASMOT.com.

70. Based on my training and experience, there is probable cause to believe that the TARGET ADDRESS contains proceeds of violations of 18 U.S.C. § 1343 (wire fraud) and property involved in violations of 18 U.S.C. §§ 1956(a)(1)(B)(i) and 1957. Specifically, as the TARGET PROPERTY is involved in money laundering it is subject to forfeiture.

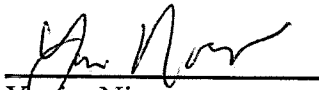
SEIZURE PROCEDURE FOR THE TARGET PROPERTY

71. Should this seizure warrant be granted, law enforcement intends to work with Tether to seize the funds associated with the Target Property. In sum, the accompanying warrant would be transmitted to Tether, at which time Tether would “burn” (i.e., destroy) the address at issue (and by extension the USDT tokens associated with it]). Tether would then reissue the equivalent amount of USDT tokens associated with the Target Property and transfer that equivalent amount of USDT to a government-controlled wallet. The seized currency will remain in the custody of the U.S. government during the entire pendency of the forfeiture proceedings,

to ensure that access to, or manipulation of, the forfeitable property cannot be made absent court order or, if forfeited to the United States, without prior consultation by the United States.

CONCLUSION

72. Based on the foregoing, I request that the Court issue the proposed seizure warrant. Because the warrant will be served on Tether.co, which accepts service by email, and Tether.co will then collect the funds at a time convenient to it and transfer the funds to the government, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.



Yanira Nieves
Special Agent
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on August 23, 2024.

Lindsey R Vaala Digitally signed by Lindsey R Vaala
Date: 2024.08.23 11:46:18 -04'00'

Lindsey R. Vaala
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A: PROPERTY TO BE SEIZED

Pursuant to this warrant, Tether shall provide the law enforcement officer/agency serving this document with the equivalent amount of USDT tokens that are currently associated with the virtual currency address referenced below (*i.e.*, **ALL USDT TOKENS ASSOCIATED WITH 0x9AFc36B20C961CD34450ae0C3941C302bfd6B1F1**]). Tether shall effectuate this process by (1) burning the USDT tokens currently associated with the virtual currency address referenced below and (2) reissuing the equivalent value of USDT tokens to a U.S. law enforcement-controlled virtual currency wallet. Tether shall provide reasonable assistance in implementing the terms of this seizure warrant and take no unreasonable action to frustrate its implementation.

- **0x9AFc36B20C961CD34450ae0C3941C302bfd6B1F1**