

**IN THE CIRCUIT COURT OF THE SEVENTEENTH JUDICIAL CIRCUIT
IN AND FOR BROWARD COUNTY, FLORIDA**

IN RE: FORFEITURE OF THE FOLLOWING
DESCRIBED PROPERTY:

Case No.

TRON WALLET ADDRESSES:

TArxGhbLdY6ApwaCYZbwdZYiHBG96heiwp,
TUNKp7upGiHt9tam37VfjHRPUUbZ1yNKS,
TVPPcD8P8QWK5eix6B6r5nVNaUFUHfUohe,
AND TCULAeahAiC9nvurUzxvusGRLD2JxoY5Yw,
CONTAINING MULTIPLE
CRYPTOCURRENCY TOKENS,

_____ /

COMPLAINT

COMES NOW, Petitioner STATE OF FLORIDA, OFFICE OF THE ATTORNEY GENERAL, DEPARTMENT OF LEGAL AFFAIRS, by and through undersigned counsel, and files this Complaint for Forfeiture by the statutory authority granted under the Florida Contraband Forfeiture Act, ("FCFA"), section 932.701-932.706, Florida Statutes and in support thereof, alleges the following:

I. NATURE OF THE ACTION

This is an action for forfeiture pursuant to the Florida Contraband Forfeiture Act ("the Act"), of certain property, to wit: Tron Wallet addresses:

TArxGhbLdY6ApwaCYZbwdZYiHBG96heiwp,
TUNKp7upGiHt9tam37VfjHRPUUbZ1yNKS,
TVPPcD8P8QWK5eix6B6r5nVNaUFUHfUohe, and
TCULAeahAiC9nvurUzxvusGRLD2JxoY5Yw

JURISDICTION AND VENUE

1. This is an action for Judgment of Forfeiture pursuant to the Florida Contraband Act under Chapter 932, Fla. Stat. Jurisdiction of this action is proper in this Court as the conduct described herein occurred in the State of Florida, the property sought to be forfeited exists in the State of Florida, is the proceeds of criminal conduct, and/or was used as an instrumentality to commit criminal conduct in the State of Florida.
2. Venue is proper in Broward County, Florida as the location of the offenses occurred within the County. § 932.704(4), Fla. Stat.

PARTIES

3. Petitioner, the State of Florida, Office of the Attorney General, Department of Legal Affairs, brings this action pursuant to the provisions of the Florida Contraband Forfeiture Act, Section 932.701- 932.706, Florida Statutes.
4. Potential Claimant Aman Kumar is believed to be the only known Claimant. The seized accounts were used to illegally launder money from a victim who reside in Broward County, Florida.

II. GENERAL ALLEGATIONS COMMON TO ALL COUNTS

5. The Fort Lauderdale Police Department is the investigative agency in this action. Affiant Jesse Gossman a Detective with the Fort Lauderdale Police Department details the facts of this case and said Affidavit is attached as **Exhibit "A"**.
6. The Fort Lauderdale Police Department received a complaint pertaining to a fraudulent transaction involving cryptocurrency coins.

VIRTUAL CURRENCY

7. “Virtual currency,” also referred to as “digital currency,” is a digital representation of value that can be digitally traded and functions as a medium of exchange, a unit of account, and a store of value. Virtual currency is neither issued nor guaranteed by any jurisdiction and fulfills these functions only by agreement within the community of users of the virtual currency. “Cryptocurrency” is a form of virtual currency that relies on cryptography to create a secure record of transactions. Cryptocurrencies are typically distributed, open-source, peer-to-peer currencies with no central administrative authority that rely on a shared computer networking protocol. “Digital asset” is a term referring to currency or cryptocurrency held in digital form.
8. Virtual currencies may be divided into two classes: “Cryptocurrency Coins” and “Digital Token”. Cryptocurrency Coins are native to their own blockchain network and may only exist on that specific blockchain network. Their value is tied solely to the market forces of the users, and they are fundamental to the operation and settlement of all transactions which occur on their blockchain network. Digital tokens are virtual currencies that are built upon an existing blockchain network and may exist on any blockchain network the developer supports.
9. Rather than acting as a traditional currency, Digital Tokens are a digitally transferable representation of some other thing of value. While Digital Tokens are tracked and secured using the decentralized cryptographic functions of the blockchain which hosts them, they are created and issued by a centralized entity. Digital Tokens are designed to provide a specific utility which provides value to the user. They may be engineered to maintain the value of a fiat currency, known as “Stablecoins”, or they may be used to track and trade ownership of a project like stock. Digital Tokens may be representative of anything the developer chooses, and their adoption and value may be dependent on the utility it provides to the market or the speculation of future value.
10. When a user acquires cryptocurrency, ownership of the cryptocurrency is transferred to the user’s “public address” on the “blockchain” for that cryptocurrency. The “public address” is somewhat analogous to a bank account number and is comprised of a string of letters and numbers that is often dozens of characters in length (depending on the cryptocurrency). All transactions for Bitcoin, and other cryptocurrencies are recorded on what is known as “blockchain.”

11. Certain blockchain networks have capabilities beyond recording simple ledger entries. These networks provide additional functionality which allows users to upload coded instructions to be performed upon a predetermined trigger. These are called Smart Contracts and once uploaded, will remain available for any user to interact with, somewhat like a virtual vending machine. When any user interacts with the Smart Contract by sending a virtual currency transaction to the Smart Contract address, the smart contract autonomously perform the function is was programmed to perform.
12. “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.
13. Tether (USDT); Tether Limited (“Tether”) is a company that manages the smart contracts and the treasure (i.e., the funds held in reserved) for USDT tokens. is a company that manages the smart contracts and the treasury (i.e., the funds held in reserve) for USDT token.
14. The “Blockchain” is essentially a distributed public ledger that keeps track of all transactions for a given cryptocurrency, incoming and outgoing, and updates regularly (multiple times per hour). The blockchain records every address that has ever received a unit of that cryptocurrency and maintains records of every transaction for each public address. This is true for Bitcoin on the Bitcoin blockchain, and Ethereum (ETH) on the Ethereum blockchain as well as many other blockchain networks. The integrity of the historical record on a blockchain is secured using cryptography and the records are built on top of one another in blocks, to verifiably ensure that no historical records can be altered.
15. While the identity of a cryptocurrency wallet address owner is generally anonymous, law enforcement can identify the owner of a particular cryptocurrency wallet address by analyzing the blockchain records. The analysis can also reveal additional cryptocurrency wallet addresses controlled by the same individual or entity.
16. When law enforcement conducts investigations involving virtual currency, they sometimes use commercial services offered by several different blockchain-analysis companies. These companies analyze the entire blockchain record coupled with additional intelligence gathering techniques to identify the individuals or groups involved in transactions. Specifically, these companies have developed proprietary software that analyzes all the

data underlying each transaction on the various blockchain networks and then groups related transactions into “clusters” based on that analysis.

17. In this particular case, the third-party blockchain-analysis software used is an anti-money laundering software used by financial institutions and law enforcement organizations worldwide. This third-party blockchain analysis software has supported many investigations and has been the basis for numerous search and seizure warrants.
18. Little to no personally identifiable information about the payer or payee is transmitted in a transaction on the blockchain. These transactions occur using a public key and a private key. A public key (reflected in the public address) is used to receive units of cryptocurrency, and a private key is used to allow withdrawals from a public address. This is done by using the private key in a cryptographic “digital signature” that provides for verification and non-repudiation, in that only a person or entity holding the private key corresponding to a given public address (public key) can provide a verifiable digital signature, and anyone in the Bitcoin or Ethereum network can use that digital signature to authenticate the transaction. Only the public address of the receiving party and the sender’s private key are needed to complete the transaction, which by themselves rarely reflects identifying information.
19. Virtual currencies, including Bitcoin and the other cryptocurrencies mentioned, have many known legitimate uses. However, much like cash, these virtual currencies can be used to facilitate illicit transactions and to launder criminal proceeds, given the ease with which they can be used to move funds with high levels of anonymity. By maintaining multiple wallets, those who use virtual currencies for illicit purposes can attempt to thwart law enforcement’s efforts to track proceeds of illicit activities. However, in some circumstances, payments using these cryptocurrencies may be traced to accounts at a cryptocurrency “exchange” or traditional financial institution using blockchain analysis.
20. A cryptocurrency “exchange,” also referred to as a Virtual Asset Service Provider “VASP” is a business that facilitates the conversion of cryptocurrency to cash or another type of cryptocurrency. An exchange typically accepts payments of fiat currency or other convertible digital currencies to obtain the desired cryptocurrency. When a user wishes to purchase bitcoins from an exchange, the user will typically send payment in the form of fiat currency, often via bank wire or ACH, or other convertible digital currency, to an

exchanger for the corresponding number of bitcoins based on a fluctuating exchange rate. The exchanger, often for a commission, will then typically attempt to broker the purchase with another user of the exchange that is trying to sell bitcoins, or, in some instances, will act as the seller itself. If the exchange can place a buyer with a seller, then the transaction can be completed. The user can then conduct transactions with other users of the cryptocurrency, by transferring bitcoins to their Bitcoin addresses, via the Internet.

21. Ownership of cryptocurrency is established through the record of transfers between public addresses on a blockchain, and private keys are used to control the transfer of assets from those addresses.
22. A cryptocurrency “wallet” is a document or piece of hardware or software that contains a set of cryptocurrency addresses and their corresponding private keys, which can be used to transfer funds from those addresses. The term “wallet” is also used to refer to an address or a collection of addresses that are controlled by the same person or entity. While cryptocurrency addresses themselves do not generally reveal the address’s owner (unless the owner opts to make information about the owner’s cryptocurrency address publicly available), the blockchain is an open distributed ledger that records transactions between two addresses efficiently and in a verifiable and permanent way. Investigators can sometimes use the blockchain to identify the owner of a particular cryptocurrency address or identify addresses that likely all belong to the same owner.
23. An NFT is a type of digital artifact that is created on and tracked through a given blockchain network. Unlike cryptocurrency tokens that can be split or combined to create various denominations, an NFT is a distinct identifiable artifact. Also, unlike cryptocurrency that is fungible, no other NFT, even if they are visually the same, can ever be substituted for another NFT as each will maintain a distinct identity. The creation of an NFT is referred to as “Minting”. The NFT transaction record acts as a certificate of authenticity and ownership for the represented digital artifact which can be sold or transferred to other users on a given blockchain. Often NFTs are digital works of art, but they may be minted to contain any other visual representation of data, creating a unique ownership and possession record.
24. Tether Operations Limited (Tether) is a Virtual Asset Service Provider and digital token issuer founded in 2014. Tether operates two distinct entities depending on the location of

the customer. Tether International Limited (TIL) is the entity that provides services for all non-US based clients. Tether Limited (TLTD) is the entity which provides services for all US persons, or any account which deposits, withdraws, or transfers assets to or from any US financial institution. The entities known collectively as Tether are considered a financial institution, as defined in 31 U.S.C. s. 5312, and are commonly referred to as a “currency exchange.”

25. A currency exchange maintains accounts and holds currency for customers and clients.
26. Tether Digital Tokens are an example of what is commonly referred to as stablecoins, in that they are engineered to maintain the value of a given fiat currency to avoid the volatility of traditional virtual currencies. Tether Digital Tokens are issued by Tether and may be tied to different virtual currencies. As of 2024, there is more than \$100 billion in circulating Tether Tokens on various blockchain networks. US Dollar Tether (USDT) maintains the value of the US dollar by holding cash reserves in audited bank accounts to back every token issued virtually on the blockchain. Users may purchase USDT directly through a user portal hosted by Tether where they exchange fiat currency for newly issued USDT or they may purchase USDT from existing USDT holders through third party exchanges or direct peer-to-peer transactions. Users may continue to transact with the USDT tokens through this manner, or they may send the USDT back to Tether to redeem it for the fiat currency.
27. Tether Smart Contract (TSC) was created by Tether on 14 different blockchain networks to facilitate the use and interoperability of Tether Digital Tokens. Anytime a user initiates a transfer of USDT (or any other Tether Digital Token) from a wallet under the user’s control to a third party (peer to peer via VASP) the Tether Smart Contract is engaged to verify the balance of the USDT changing custody and permit the transfer of value from the sending wallet address to the receiving wallet address.
28. The Tether Smart Contract is under the direct control of Tether and acts as a centralized gatekeeper to permit and facilitate the transfer of Tether Digital Tokens; even between decentralized anonymous third parties. Tether maintains the technical ability to place specific wallet addresses on a blacklist which will revoke their ability to interact with Tether Smart Contract. In effect, this will trap the total balance of all Tether Digital Tokens in the identified wallet indefinitely. This process is known as “burning” the Tether Digital Tokens. Tether may then “reissue” newly created Tether Digital Tokens to replace the

“burned” tokens and assign ownership to a predetermined Tether platform user account or government-controlled cryptocurrency wallet address.

III. ALLEGATIONS

29. An investigation was conducted by the Fort Lauderdale Police Department investigating the scams committed on a resident of Broward County.
30. Ms. Berdugo (VICTIM 1), a Broward County resident) advised the Fort Lauderdale Police Department that back on October 31, 2023, she received a pop-up window on her Apple computer which stated her account had been hacked and instructed her to contact the provided phone number for assistance.
31. VICTIM 1 called the number provided and spoke with whom she believed to be an Apple help desk representative. The representative then had VICTIM1 share access to her computer under the guise of helping to resolve the problem. The “representative” then appeared to log into her Wells Fargo account where her screen displayed a charge for \$43,000 to Porn Hub.
32. The representative then stated that he would connect her on a three-way call to a “Wells Fargo representative” that could help her with the unauthorized charge. The “Wells Fargo representative” then told the victim that the charges appeared to be associated with child pornography and that she could face criminal charges if the transaction went through. He explained to VICTIM 1 that the charges were still “pending”.
33. VICTIM 1 was instructed to withdraw the funds from her account in cash then convinced her to secure them in the bank’s cryptocurrency wallet where the funds

would be credited to a new account opened for her the next day.

34. VICTIM 1 was then directed by address to the banks where she should make the withdrawals and crypto kiosks to make the deposits.
35. VICTIM 1 made three separate deposits (10/31/2023 \$21,500; 10/31/2023 \$9,800.00; and 10/31/2023 \$11,000) totaling \$42,300 into various crypto kiosks within the city of Fort Lauderdale.
36. A blockchain analysis for VICTIM 1's deposits identified two additional victims which also paid into the same criminal network of wallet addresses. These assets were combined and laundered with one another.
37. Garland Erguden (VICTIM 2), a resident of Memphis, Tennessee made two other deposits representing a total theft of \$41,500.
38. Just like VICTIM 1, VICTIM 2 received a pop up on her computer which stated they compromised and would need to call a helpdesk number. Once she contacted the number, she was told that there had been a \$42,000 payment to "childporn.com". VICTIM 2 was directed to withdraw the cash from their bank to prevent the payment and deposit into the bank's crypto wallet using a crypto kiosk. VICTIM 2 contacted the Memphis Police Department.
39. Brett Baines (VICTIM 3) a resident of Renton, Washington made a deposit of \$10,500 into a Bitcoin ATM on 11/27/2023 which resulted in the purchase and transfer of .216 BTC to wallets under control of the criminal network.
40. VICTIM 3 was hesitant to speak on the phone as he confirmed he had been scammed and no further details were provided.
41. Mohamed Shehata (VICTIM 4) a resident of Hamilton, New Jersey received a notice

on his computer from Apple Support. The notice advised him to contact a representative at the provided number. VICTIM 4 was told that his computer had been compromised resulting in transactions to Pornhub from his bank account.

42. VICTIM 4 allowed access to his computer to the person representing themselves as Apple Support which resulted in his Robinhood crypto account being compromised. The suspects made two separate transfers of ETH totaling 2.1 ETH to a wallet address under the control of the criminal network.

43. VICTIM 4 filed a report with the Hamilton Police Department on 11/8/2023.

44. All analysis was performed for the purpose of identifying the flow of VICTIM 1's assets. All tracing is conducted in accordance with a Proceeds-In-First-Out (PIFO) tracing methodology unless articulable facts exist for a deviation from PIFO.

45. There is only one such deviation in this trace where the "matching transactions" principle is applied. This is due to incoming and outgoing transactions which are specific in amount and close in time where the inference is made that the inflow and outflow of assets were intended to move the specified assets.

46. There were three separate deposits originating from VICTIM 1 and arriving on the Bitcoin blockchain network. Each of these deposits were commingled with additional deposits from other crypto kiosks from other suspected victims.

47. All assets were consolidated into 2.8 BTC and sent to Fixed Float (a hosted, non-custodial exchange). Records from Fixed Float identified that the stolen BTC was converted to USDT and bridged (transferred) to the Tron network.

48. The stolen assets can be traced from the deposit at the crypto kiosk, through five (5) intermediary wallets before arriving at Fixed Float exchange. Each of these

transactions represent the proceeds of a specified unlawful activity and are designed to conceal the source, ownership, and control of the proceeds of unlawful activity.

49. Once the assets arrive at Fixed Float exchange, the path of the assets is no longer publicly visible on the Bitcoin blockchain.

50. The investigator made an official request to Fixed Flow exchange and received the business records necessary to identify the conversion and destination of the assets traceable to the initial theft.

51. The investigation revealed that upon entering the Tron network, the criminal proceeds took two distinct forks. Fork 1 arrived on Tron as an 86,429.86 USDT transaction and originated from a 2.5 BTC UTXO comprised of .78 BTC traced directly to VICTIM 1 deposits 1, 2, and 3 under hash bb6767f979332d0bbd366c6445e3a5738cacle8cclc09607c50dc5c382a5164. The remainder of the 2.5 traced to other crypto kiosk deposits from additional potential victims.

52. Fork 1a shows Applying the Proceeds-In-First-Out (PIFO) tracing method, from there, 65,000 USDT is sent through an intermediary wallet before being split. A 30,000 USDT transaction continues through one additional wallet before being comingled with numerous other deposits. Those other USDT deposits are consolidated and set to wallet address TMX7iCSEuE4EZaUm13FKDwV2GUwG3ASF8M as a portion of the 1,371.782 USDT deposit.

53. This address continued to get additional deposits and is split again into a 1,151,376 USDT transfer to wallet **TArxGhbLdY6ApwaCYZbwdZYiHBG96heiwp** (Target

Property 1) with transaction has
0x11ce9a16b8d9596bcfbab824cc26de72d5639118890ac0ad169cdf1bef33100b; and
a 619,973.34 USDT transaction to wallet
TUNKp7upGiHt9tamt37VfjHRPUUbZ1yNKS (Target Property 2) under
transaction
0x710cd81cb45875432677453bf2c0ef758b865d0dbe53e5e91b9f7ede6dfd96f4.

54. These wallet addresses are being used as an instrumentality to the crime of money laundering and contain proceeds directly traceable to VICTIM 1 deposits 1, 2, and 3 as well as VICTIM 2.

55. After Fork 1a occurred the remaining 21,606 USDT attributed to the Fixed Float transaction was sent as the majority of a 22,985 YSDT transfer to wallet address **TVPPcD8P8QWK5eix6B6r5nVNaUFUHfUohe** (Target Account 3). The remaining balance of the transaction was proceeds of a theft attributed to VICTIM 2.

56. Fork 2 arrived on Tron as .133 BTC originating from VICTIM 1 deposit 2 as a portion of a 10.345.15 USDT transaction containing assets of the other suspected victims under hash
0xe79d02cf74b11afe02c4daa41f3129af11668d3751a7458daa7d6974086cfe7d.

57. Once the Tron network, the exact amount of 10,346 is moved to another wallet within 24 hours (due to the precise amount and proximity in time, PIFO tracing method was substituted for the matching transactions principle).

58. Fork 2 arrived on Tron as 10.346.15 USDT transaction and originated from a .3 BTC UTXO comprised of .133 BTC traced directly to VICTIM 1 deposit 2.

59. Once on the Tron network, the exact amount of 10.346 is moved to another wallet within 24 hours (due to the precise amount and proximity in time, FIFO tracing method was substituted for the matching transactions principle).
60. There was then an 8,000 USDT transaction transferred to a wallet in the Fork 1b path where it was commingled with other assets and abandoned for the purposes of tracing.
61. The remaining 2,346 USDT originating from the Fixed Float transaction directly traceable to VICTIM 1 deposit 2 was transferred to wallet address **TCULAeahAiC9nvurUzxvusGRLD2JxoY5Yw** (Target Account 4) as a portion of a 25,850 USDT deposit.
62. The remaining balance of that transaction are proceeds directly traceable to VICTIM 3.
63. These funds were then comingled with existing assets in the wallet which has a current balance of 276,966 USDT.
64. This wallet is being used as an instrumentality to the crime of money laundering and contains proceeds directly traceable to VICTIM 1 deposit 2 as well as VICTIM 3.
65. The financial transactions involved in the above-described blockchain analysis are indicative of an orchestrated attempt by a single criminal enterprise or entity to conceal the source and ownership of criminal proceeds. Despite the use of various wallet addresses and obfuscation techniques, the assets remained under the control of the criminal enterprise from the time of the initial theft and the placement of assets into the virtual asset eco system, through the layering process to the wallet addresses identified as Target Properties 1-4.

66. Aman Kumar contacted Tether through an email exchange regarding the investigation. The investigator conducted a diligent search of the provided name and email address but was not able to identify further contact information.
67. The investigation included research into the IP addresses identified via business records used to transfer assets through the Fixed Float exchange. The exchange transactions for VICTIM 1 and VICTIM 2 originated from Chandigarh India and the exchange transaction for VICTIM 3 originated in Mumbai India.
68. The funds were seized on May 8, 2025, and on May 9, 2025, a Notice of Seizure was sent via email to the only known possible claimant at lamankumar@myyahoo.com. (See Exhibit “B”).
69. Based on the totality of the circumstances, the TRON WALLET ADDRESSES:

**TArxGhbLdY6ApwaCYZbwdZYiHBG96heiwp,
TUNKp7upGiHt9tam37VfjHRPUUbZ1yNKS,
TVPPcD8P8QWK5eix6B6r5nVNaUFUHfUohe, and
TCULAeahAiC9nvurUzxvusGRLD2JxoY5Yw,**

containing multiple cryptocurrency tokens, was seized for forfeiture as there is probable cause to believe that it was contraband under the Florida Contraband Forfeiture Act by totality of the circumstances demonstrating a nexus between the currency and Chapter 812, 817, and 896 theft, fraud, and money laundering violations, in that the currency had been stolen from a Florida victim, transported, and converted to cryptocurrency in an effort to conceal the ultimate use of funds.

COUNT 1

VIOLATION OF THE FLORIDA CONTRABAND FORFEITURE ACT, § 932.702(2), FLA. STAT.

1. Petitioner incorporates herein the allegations contained in paragraphs 1-69.

2. Potential Claimant, Aman Kumar concealed or possessed TRON accounts associated with **TArxGhbLdY6ApwaCYZbwdZYiHBG96heiwp**, **TUNKp7upGiHt9tam37VfjHRPUUbZ1yNKS**, **TVPPcD8P8QWK5eix6B6r5nVNaUFUHfUohe**, and **TCULAeahAiC9nvurUzxvusGRLD2JxoY5Yw**. The accounts and their contents were used or was attempted to be used as an instrumentality in the commission of, or in aiding or abetting in the commission of a Felony, including but not limited to Scheme to Defraud pursuant to Florida Statutes section 817.034(40)(a)(2); Grand Theft pursuant to Florida Statutes section 812.014(2)(b)(1); Money Laundering pursuant to Florida Statutes section 896.103 and Fraud pursuant to Florida Statutes section 560.111(2) in violation of *§ 932.702(2), Fla. Stat.*

WHEREFORE, the Petitioner hereby requests this Court to grant Judgment as follows: finding the property described as: TRON accounts associated with **TArxGhbLdY6ApwaCYZbwdZYiHBG96heiwp**, **TUNKp7upGiHt9tam37VfjHRPUUbZ1yNKS**, **TVPPcD8P8QWK5eix6B6r5nVNaUFUHfUohe**, and **TCULAeahAiC9nvurUzxvusGRLD2JxoY5Yw**, is contraband under the FCFA, transferring all rights, title, and ownership in the seized items to the State of Florida Office of the Attorney General, Department of Legal Affairs and/or the Florida Department of Law Enforcement; award Petitioner attorneys' fees and costs reasonably incurred for the investigation and litigation of the above claims; and all other relief this Court deems just and proper.

COUNT 2

VIOLATION OF THE FLORIDA CONTRABAND FORFEITURE ACT,

§ 932.702(3), FLA. STAT.

3. Petitioner incorporates herein the allegations contained in paragraphs 1-69.

4. Potential Claimant, Aman Kumar used TRON accounts associated with

TArxGhbLdY6ApwaCYZbwdZYiHBG96heiwp,

TUNKp7upGiHt9tam37VfjHRPUUbZ1yNKS,

TVPPcD8P8QWK5eix6B6r5nVNaUFUHfUohe, and

TCULAeahAiC9nvurUzxvusGRLD2JxoY5Yw to facilitate the transportation,

carriage, conveyance, concealment, receipt, possession, purchase, sale, barter, exchange,

or giving away of money, securities, records, negotiable instruments, currency including

virtual currency. The account and its contents was used or was attempted to be used as an

instrumentality in the commission of, or in aiding or abetting in in the commission of a

Felony, including but not limited to Scheme to Defraud pursuant to Florida Statutes

section 817.034(40)(a)(2); Grand Theft pursuant to Florida Statutes section

812.014(2)(b)(1); Money Laundering pursuant to Florida Statutes section 896.103 and

Fraud pursuant to Florida Statutes section 560.111(2) in violation of § 932.702(3), *Fla.*

Stat.

WHEREFORE, the Petitioner hereby requests this Court to grant Judgment as follows:

finding the property described as: TRON accounts associated with

TArxGhbLdY6ApwaCYZbwdZYiHBG96heiwp,

TUNKp7upGiHt9tam37VfjHRPUUbZ1yNKS,

TVPPcD8P8QWK5eix6B6r5nVNaUFUHfUohe, and

TCULAeahAiC9nvurUzxvusGRLD2JxoY5Yw is contraband under the FCFA,

transferring all rights, title, and ownership in the seized items to the State of Florida Office of

the Attorney General, Department of Legal Affairs and/or the Florida Department of Law Enforcement; award Petitioner attorneys' fees and costs reasonably incurred for the investigation and litigation of the above claims; and all other relief this Court deems just and proper.

COUNT 3
VIOLATION OF THE FLORIDA CONTRABAND FORFEITURE ACT,
§932.702(4)

5. Petitioner incorporates herein the allegations contained in paragraphs 1-69.
6. Potential Claimant, Aman Kumar concealed, possessed or used TRON accounts associated with **TArxGhbLdY6ApwaCYZbwdZYiHBG96heiwp,**
TUNKp7upGiHt9tam37VfjHRPUUbZ1yNKS,
TVPPcD8P8QWK5eix6B6r5nVNaUFUHfUohe, and
TCULAeahAiC9nvurUzxvusGRLD2JxoY5Yw as an instrumentality in the commission of, or in aiding or abetting in the commission of a Felony, including but not limited to Scheme to Defraud pursuant to Florida Statutes section 817.034(40)(a)(2); Grand Theft pursuant to Florida Statutes section 812.014(2)(b)(1); Money Laundering pursuant to Florida Statutes section 896.103 and Fraud pursuant to Florida Statutes section 560.111(2) in violation of § 932.702(4), *Fla. Stat.*

WHEREFORE, the Petitioner hereby requests this Court to grant Judgment as follows:
finding the property described as: TRON accounts associated with

TArxGhbLdY6ApwaCYZbwdZYiHBG96heiwp,
TUNKp7upGiHt9tam37VfjHRPUUbZ1yNKS,
TVPPcD8P8QWK5eix6B6r5nVNaUFUHfUohe, and
TCULAeahAiC9nvurUzxvusGRLD2JxoY5Yw is contraband under the FCFA,

transferring all rights, title, and ownership in the seized items to the State of Florida Office of the Attorney General, Department of Legal Affairs and/or the Florida Department of Law Enforcement; award Petitioner attorneys' fees and costs reasonably incurred for the investigation and litigation of the above claims; and all other relief this Court deems just and proper.

IV. **RELIEF SOUGHT**

WHEREFORE, Petitioner prays for this Court to enter its Final Judgment in its favor as well as the following relief:

- a. Enjoin Claimants, individually and/or by or through their spouses, family members, power of attorney, trustees, agents, employees, or other persons, from transferring, conveying, encumbering, disposing of or otherwise alienating the property identified above.
- b. Enter Final Judgment of Forfeiture perfecting the right to, and title and interest in subject property, to the Petitioner, the State of Florida Office of the Attorney General, Department of Legal Affairs and/or the Florida Department of Law Enforcement.
- c. Award attorneys' fees and costs reasonably incurred for the investigation and litigation of the above claims.
- d. Order the forfeiture of any other property of the claimant up to the value of any property subject to forfeiture under this section if any of the property: cannot be located; Has been transferred to, sold to, or deposited with, a third party; Has been placed beyond the jurisdiction of the court; Has been substantially diminished in value by any act or omission of the person in possession of the property; or Has

been commingled with any property which cannot be divided without difficulty pursuant to § 932.703(6).

DEMAND FOR JURY TRIAL

Petitioner demands a trial by jury.

Dated: May 28, 2025

Respectfully submitted,

**JAMES UTHMEIER
ATTORNEY GENERAL**

/s/ Kathleen M. Savor

Kathleen M. Savor

Litigation Forfeiture Manager

Florida Bar No. 139114

Office of the Attorney General

110 S. E. 6th Street, 10th Floor

Fort Lauderdale, Florida 33301

Telephone: (954) 712-4611

Facsimile: (954) 527-3702

Kathleen.Savor@myfloridalegal.com

EXHIBIT A

COUNT II

ORGANIZED FRAUD in violation of FSS 817.034-4a1

COUNT III

GRAND THEFT >\$20,000 in violation of F.S.S. 812.014-2b1

COUNT IV

DEALING IN STOLEN PROPERTY in violation of F.S.S. 812.019-1

BACKGROUND RELATED TO VIRTUAL CURRENCY

I. Bitcoin and other Cryptocurrencies

1. "Virtual currency," also referred to as "digital currency," is a digital representation of value that can be digitally traded and functions as a medium of exchange, a unit of account, and a store of value. Unlike fiat currency, (currency which derives its value from government regulation or law,) virtual currency is neither issued nor guaranteed by any jurisdiction and fulfills these functions only by agreement within the community of users of the virtual currency. "Cryptocurrency" is a form of virtual currency that relies on cryptography to create a secure record of transactions. Cryptocurrencies are typically distributed, open-source, peer-to-peer currencies with no central administrating authority that rely on a shared computer networking protocol. "Digital asset" is a term referring to currency or cryptocurrency held in digital form.
2. Virtual currencies may be divided into two classes; "Cryptocurrency Coins" and "Digital Tokens". Cryptocurrency Coins are native to their own blockchain network and may only exist on that specific blockchain network. Their value is tied solely to the market forces of the users, and they are fundamental to the operation and settlement of all transactions which occur on their blockchain network. Digital tokens are virtual currencies that are built upon an existing blockchain network and may exist on any blockchain network the developer supports. Rather than acting as a traditional currency, Digital Tokens are a digitally transferable representation of some other thing of value. While Digital Tokens are tracked and secured using the decentralized cryptographic functions of the blockchain which hosts them, they are created and issued by a centralized entity. Digital Tokens are designed to provide a specific utility which provides value to the user. They may be engineered to maintain the value of a fiat currency, known as "Stablecoins", or they may be used to track and trade ownership of a project like stock. Digital Tokens may be representative of anything the developer chooses, and their adoption and value may be dependent on the utility it provides to the market or the speculation of future value.
3. When a user acquires cryptocurrency, ownership of the cryptocurrency is transferred to the user's "public address" on the "blockchain" for that cryptocurrency. The "public address" is somewhat analogous to a bank account number and is comprised of a string of letters and numbers that is often dozens of characters in length (depending on the cryptocurrency).

All transactions for Bitcoin, and other cryptocurrencies are recorded on what is known as a “blockchain.”

4. **Smart Contracts.** Certain blockchain networks have capabilities beyond recording simple ledger entries. These networks provide additional functionality which allows users to upload coded instructions to be performed upon a predetermined trigger. These are called Smart Contracts and once uploaded, will remain available for any user to interact with, somewhat like a virtual vending machine. When any user interacts with the Smart Contract by sending a virtual currency transaction to the Smart Contract address, the smart contract will autonomously perform the function it was programmed to perform.
5. **“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, USDC 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.
6. **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.

II. Blockchain Analysis

1. The “Blockchain” is essentially a distributed public ledger that keeps track of all transactions for a given cryptocurrency, incoming and outgoing, and updates regularly (multiple times per hour). The blockchain records every address that has ever received a unit of that cryptocurrency and maintains records of every transaction for each public address. This is true for Bitcoin on the Bitcoin blockchain, and Ethereum (ETH) on the Ethereum blockchain as well as many other blockchain networks. The integrity of the historical record on a blockchain is secured using cryptography and the records are built on top of one another in blocks, to verifiably ensure that no historical records can be altered.
2. As previously stated, while the identity of a cryptocurrency wallet address owner is generally anonymous, law enforcement can identify the owner of a particular cryptocurrency wallet address by analyzing the blockchain records. The analysis can also reveal additional cryptocurrency wallet addresses controlled by the same individual or entity. For example, a user or business may create many Bitcoin addresses to receive payments from different customers. When the user wants to transact the bitcoin that he or she has received (*e.g.*, to exchange bitcoin for other currency or to use bitcoin to purchase goods or services), the user may group those addresses together to send a single transaction.
3. When law enforcement conducts investigations involving virtual currency, they sometimes use commercial services offered by several different blockchain-analysis companies. These companies analyze the entire blockchain record coupled with additional intelligence gathering techniques to identify the individuals or groups involved in transactions. Specifically, these companies have developed proprietary software that analyzes all the

data underlying each transaction on the various blockchain networks and then groups related transactions into “clusters” based on that analysis. The methods employed by these blockchain analysis companies have been independently validated by computer scientists, who have shown that these “clustering” techniques provide accurate results. Additionally, through numerous, unrelated investigations, law enforcement has been able to corroborate the accuracy of the information provided via these third-party services.

4. The third-party blockchain-analysis software utilized in the instant case is an anti-money laundering software used by financial institutions and law enforcement organizations worldwide. This third-party blockchain analysis software has supported many investigations and has been the basis for numerous search and seizure warrants.
5. Little to no personally identifiable information about the payer or payee is transmitted in a transaction on the blockchain. These transactions occur using a public key and a private key. A public key (reflected in the public address) is used to receive units of the cryptocurrency, and a private key is used to allow withdrawals from a public address. This is done by using the private key in a cryptographic “digital signature” that provides for verification and non-repudiation, in that only a person or entity holding the private key corresponding to a given public address (public key) can provide a verifiable digital signature, and anyone in the given blockchain network can use that digital signature to authenticate the transaction. Only the public address of the receiving party and the sender’s private key are needed to complete the transaction, which by themselves rarely reflect any identifying information.
6. Virtual currencies, including Bitcoin and the other cryptocurrencies mentioned, have many known legitimate uses. However, much like cash, these cryptocurrencies can be used to facilitate illicit transactions and to launder criminal proceeds, given the ease with which they can be used to move funds with high levels of anonymity. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement’s efforts to track proceeds of illicit activities. However, in some circumstances, payments using these cryptocurrencies may be traced to accounts at a cryptocurrency “exchange” or traditional financial institution using blockchain analysis.

III. Cryptocurrency Exchange

1. A cryptocurrency “exchange,” also referred to as a Virtual Asset Service Provider “VASP,” is a business that facilitates the conversion of cryptocurrency to cash or another type of cryptocurrency. An exchange typically accepts payments of fiat currency or other convertible digital currencies to obtain the desired cryptocurrency. When a user wishes to purchase, for example, bitcoins from an exchange, the user will typically send payment in the form of fiat currency, often via bank wire or ACH, or other convertible digital currency, to an exchange for the corresponding number of bitcoins based on a fluctuating exchange rate. The exchange, often for a commission, will then typically attempt to broker the purchase with another user of the exchange that is trying to sell bitcoins, or, in some instances, will act as the seller itself. If the exchange can place a buyer with a seller, then

the transaction can be completed. The user can then conduct transactions with other users of the cryptocurrency, by transferring bitcoins to their Bitcoin addresses, via the Internet. As described above, ownership of cryptocurrency is established through the record of transfers between public addresses on a blockchain, and private keys are used to control the transfer of assets from those addresses.

IV. Cryptocurrency Wallet

A cryptocurrency "wallet" is a document or piece of hardware or software that contains a set of cryptocurrency addresses and their corresponding private keys, which can be used to transfer funds from those addresses. The term "wallet" is also used to refer to an address or a collection of addresses that are controlled by the same person or entity. While cryptocurrency addresses themselves do not generally reveal the address's owner (unless the owner opts to make information about the owner's cryptocurrency address publicly available), the blockchain is an open, distributed ledger that records transactions between two addresses efficiently and in a verifiable and permanent way. Investigators can sometimes use the blockchain to identify the owner of a particular cryptocurrency address or identify addresses that likely all belong to the same owner. For example, because these blockchains serve as a searchable public ledger of every transaction, investigators can trace transactions to other cryptocurrency public addresses, including cryptocurrency exchanges and cryptocurrency payment processors.

V. Non Fungible Token (NFT)

A NFT is a type of digital artifact that is created on and tracked through a given blockchain network. Unlike cryptocurrency tokens that can be split or combined to create various denominations, a NFT is a distinct identifiable artifact. Also unlike cryptocurrency that is fungible, no other NFT, even if they are visually the same, can ever be substituted for another NFT; as each will maintain a distinct identity. The creation of a NFT is referred to as "Minting". The NFT transaction record acts as a certificate of authenticity and ownership for the represented digital artifact which can be sold or transferred to other users on a given blockchain. Often NFT's are digital works of art, but they may be minted to contain any other visual representation of data, creating a unique ownership and possession record.

BACKGROUND RELATED TO TETHER LIMITED

1. Tether Operations Limited (Tether) is a Virtual Asset Service Provider and digital token issuer founded in 2014 and based in the British Virgin Islands. Tether maintains a registered address of [REDACTED] British Virgin Islands". Tether operates two distinct entities depending on the location of the customer. Tether International Limited (TIL) maintains the same registered address as Tether. TIL is the entity which provides services for all non-US based clients. Tether Limited (TLTD) maintains the same registered address as Tether. TLTD is the entity which provides services for all US persons, or any account which deposits, withdraws, or transfers assets to or from any US financial institution. The entities known collectively as Tether are considered a financial institution, as defined in 31 U.S.C. s. 5312, and are commonly

referred to as a “currency exchange.” A currency exchange maintains accounts and holds currency for customers and clients.

2. Tether Digital Tokens are an example of what is commonly referred to as stablecoins, in that they are engineered to maintain the value of a given fiat currency to avoid the volatility of traditional virtual currencies. Tether Digital Tokens are issued by Tether and may be tied to different fiat currencies. As of 2024 there is more than \$100 billion in circulating Tether Tokens on various blockchain networks. US Dollar Tether (USDT) maintains the value of the US dollar by holding cash reserves in audited bank accounts to back every token issued virtually on the blockchain. Users may purchase USDT directly through a user portal hosted by Tether where they exchange fiat currency for newly issued USDT or they may purchase USDT from existing USDT holders through third party exchanges or direct peer to peer transactions. Users may continue to transact with the USDT tokens through this manner or they may send the USDT back to Tether to redeem it for the fiat currency.
3. Tether Smart Contract (TSC). Tether has created Smart Contracts on 14 different blockchain networks to facilitate the use and interoperability of Tether Digital Tokens. Anytime a user initiates a transfer of USDT (or any other Tether Digital Token) from a wallet under the user’s control to a third party (peer to peer or via VASP) the Tether Smart Contract is engaged to verify the balance of the USDT changing custody and permit the transfer of value from the sending wallet address to the receiving wallet address.
4. Burn and Reissue of Tether Digital Tokens. The Tether Smart Contract is under the direct control of Tether and acts as a centralized gatekeeper to permit and facilitate the transfer of Tether Digital Tokens; even between decentralized anonymous third parties. Tether maintains the technical ability to place specific wallet addresses on a blacklist which will revoke their ability to interact with the Tether Smart Contract. In effect, this will trap the total balance of all Tether Digital Tokens in the identified wallet indefinitely. This process is known as “burning” the Tether Digital Tokens. Tether may then “reissue” newly created Tether Digital Tokens to replace the “burned” tokens and assign ownership to a predetermined Tether platform user account or government controlled cryptocurrency wallet address.

PROPERTY SOUGHT

Unidentified USDT user(s) possessing the private keys to Tron Network Wallet Addresses maintain such accounts assigned to “**TArxGhbLdY6ApwaCYZbwdZYiHBG96heiwp** (Target Property #1), **TUNKp7upGiHt9tamt37VfjHRPUUbZ1yNKS** (Target Property #2), **TVPPcD8P8QWK5eix6B6r5nVNaUFUHfUohe** (Target Property #3), and **TCULAcAhAiC9nvurUzxvusGRLD2JxoY5Yw** (Target Property #4).

Within these accounts there exists the below-described property, which was used as a means to commit a crime, or which constitutes evidence relevant to proving felonies have been committed, and/or are proceeds from criminal activity or unlawfully obtained funds located in Broward County, Florida, to wit:

1. Target Property 1
Tron Network Address TArxGhbLdY6ApwaCYZbwdZYiHBG96heiwp
Asset Balance: 1,052,556.24 USDT (as of 5/6/2025)
2. Target Property 2
Tron Network Address TUNKp7upGiHt9tamt37VfjHRPUUbZ1yNKS
Asset Balance: 661,930.31 USDT (as of 5/6/2025)
3. Target Property 3
Tron Network Address TVPPcD8P8QWK5eix6B6r5nVNaUFUHfUohe
Asset Balance: 45,835.79 USDT (as of 5/6/2025)
4. Target Property 4
Tron Network Address TCULAeahAiC9nvurUzxvusGRLD2JxoY5Yw
Asset Balance: 276,966.14 USDT (as of 5/6/2025)

AFFIANT'S QUALIFICATIONS

1. Your Affiant, Detective Jesse Gossman is a duly sworn law enforcement officer currently employed by the Fort Lauderdale Police Department. Your Affiant has been a law enforcement officer for approximately eight-teen (18) years. Your affiant is currently assigned to the Economic Crimes Unit at the Fort Lauderdale Police Department and has been for approximately twelve (12) years. Your affiant has personally conducted numerous fraud and crypto related investigations during his law enforcement career. Your affiant has a master's degree in forensic accounting, holds professional designations of Certified Fraud Examiner, Certified Economic Crimes Forensic Examiner, Certified Digital Currency Investigator, Cryptocurrency Tracing Certified Examiner, TRM Advanced Crypto Investigator and has completed hundreds of hours in state, local and federal law enforcement training environments concerning money laundering and virtual currency investigations.

PROBABLE CAUSE

1. The suspect did conduct financial transactions knowing that the property involved (various virtual currencies) represented proceeds of criminal activity and did conduct such financial transactions with intent to promote the carrying on of the illegal activity. The suspect also did so, knowing that the transactions were designed to conceal the control and location of the proceeds from the criminal activity.
2. The suspect did engage in a scheme to defraud and did thereby obtain property from the victim with an aggregate value of \$42,300 US dollars.
3. The suspect did knowingly obtain the property of another person with intent to permanently deprive the owner of the right and benefit of that property through three separate transactions which occurred within the jurisdictional limits of the City of Fort Lauderdale:
 - a. 10/31/23 - \$21,500
 - b. 10/31/23 - \$9,800
 - c. 10/31/23 - \$11,000

4. The suspect did knowingly traffic in property that they knew or should have known was stolen in violation of law.

To wit:

On or about October 31, 2023, Ms. Berdugo (VICTIM 1), a resident of Broward County FL, received a pop-up window on her Apple computer which stated her account had been hacked and instructed her to contact the provided phone number for assistance. Victim 1 called the number provided and spoke with whom she believed to be an Apple help desk representative. The representative then had Victim 1 share access to her computer under the guise of helping to resolve the problem. The "representative" then appeared to log into her Wells Fargo account where her screen displayed a charge for \$43,000 to Porn Hub. The representative then stated that he would connect her on a three-way call to a "Wells Fargo representative" that could help her with the unauthorized charge. The "Wells Fargo representative" then told the victim that the charges appeared to be associated with child pornography and that she could face criminal charges if the transaction went through. He explained to Victim 1 that the charges were still "pending". In order to prevent the transaction from going through he instructed her to withdraw the funds from her account in cash. He then convinced her to secure them in the bank's cryptocurrency wallet where the funds would be credited to a new account opened for her the next day. She was then directed by address to the banks where she should make the withdrawals and crypto kiosks to make the deposits. She deposited funds totaling \$42,300 into various crypto kiosks within the city of Fort Lauderdale. Victim 1 made the following deposits:

Victim 1 (Florida Resident) Deposits:

| Victim Deposit | Amount | Date | Hash |
|----------------|-------------|----------|--|
| 1 | .251 BTC | 10/31/23 | 49e0f9e4a8112ae0ff6df55bd4ce0622f1bb0be3b8b9eccc6c8a49adde03514a |
| 2 | .203 BTC | 10/31/23 | 7afc0635ae316f44ce96bb1c89e7fec67c8b4a69c3a8efc6cbfe79b7da5273f3 |
| 3 | .467 BTC | 10/31/23 | dd6df6879e85ce8fd403b7222f33f46616a0df795fb6849f2bcedfa83d24b9c5 |

Deposit 1 \$21,500 USD occurred at [REDACTED] Fort Lauderdale FL

Deposit 2 \$9,800 USD occurred at [REDACTED] Fort Lauderdale FL

Deposit 3 \$11,000 USD occurred at [REDACTED] Fort Lauderdale FL

Upon conducting the blockchain analysis (described below) for VICTIM 1's deposits, in an attempt to account for additional assets commingled with VICTIM 1's assets, your affiant identified three additional victims which also paid into the same criminal network of wallet addresses. These assets were commingled and laundered with one another.

Victim 2 (Tennessee Resident) Deposit:

| Victim Deposit | Amount | Date | Hash |
|----------------|-------------|----------|--|
| 1 | .325 BTC | 10/24/23 | 55184bc2f735e81392952ff429273b351237e95e95e8d937278cead56e3d17c9 |
| | | | |

Deposit 1 \$14,300 USD occurred at [REDACTED] Memphis TN.

In addition to deposit 1 listed above, which was directly commingled with VICTIM 1's assets, Garland Erguden, a resident of Memphis Tennessee, (VICTIM 2) made two other deposits representing a total theft of \$41,500, Just as with VICTIM 1, VICTIM 2 received a pop up on her computer which stated she was compromised and would need to call a helpdesk number. Once she contacted the number, she was told that there had been a \$42,000 payment to "childporn.com". She was directed to withdraw the cash from her bank to prevent the payment and deposit into the bank's crypto wallet using a crypto kiosk. Erguden later filed a police report on 10/25/23 with the Memphis police Dept. under case number 2310030671ME. **Victim 3**

(Washington Resident) Deposit:

| Victim Deposit | Amount | Date | Hash |
|----------------|-------------|----------|--|
| 1 | .216 BTC | 11/27/23 | d9e764223e35f4a6bd62595aad67f6cf94f4bef90cfceb030901659cd2d7d62f |

Deposit 1 \$10,500 USD occurred at [REDACTED] Renton, WA

Brett Baines, a resident of Renton, Washington (VICTIM 3) made a deposit of \$10,500 into a BTC ATM on 11/27/23 which resulted in the purchase and transfer of .216 BTC to wallets under control of the criminal network. Your affiant later attempted to obtain additional details on the reason for the transaction, but Baines was hesitant to speak over the phone as he confirmed he had been scammed. Baines did not provide any further details on how he had been scammed.

Victim 4 (New Jersey Resident) Deposit:

| Victim Deposit | Amount | Date | Hash |
|----------------|-------------|-----------|--|
| 1 | 1.61 ETH | 11/7/2023 | 0xc7ab5130bfd2d665b67f47e131c91fd2afa16453bae4277b09dc8f2e0743cc03 |
| 2 | .528 ETH | 11/7/2023 | 0xaaa6bc9fa3bb5ce10df542c16cdf00c9449d811b730e8cbb7c0fc3d69987dd7c |

Mohamed Shehata, a resident of Hamilton, New Jersey (VICTIM 4) received a notice on his computer from Apple Support. The notice advised him to contact a representative at the provided number. Upon doing so he was told that his computer had been compromised resulting in transactions to Pornhub from his bank account. Shehata allowed access to his computer to the person representing themselves as Apple Support which resulted in his Robinhood crypto account being compromised. The suspects made two separate transfers of Eth totaling 2.1 ETH (approximately \$4,000 on the date of theft) to a wallet address under the control of the criminal

of a specified unlawful activity and are designed to conceal the source, ownership, and control of the proceeds of unlawful activity.

Upon entering the Tron network, the criminal proceeds took two distinct forks. Fork 1 arrived on Tron as a 86,429.86 USDT transaction and originated from a 2.5 BTC UTXO comprised of .78 BTC traced directly to VICTIM 1 deposits 1, 2, and 3. The remainder of the 2.5 was traced to other crypto kiosk deposits from additional potential victims. Fork 2 arrived on Tron as 10,346.15 USDT transaction and originated from a .3 BTC UTXO comprised of .133 BTC traced directly to VICTIM 1 deposit 2.

Fork 1

The 2.5 BTC (approx. \$87,289 at time of transaction) containing proceeds directly traceable to VICTIM 1 deposits 1, 2, and 3 (comingled with other crypto kiosk victims) arrived on Tron as a 86,429.86 USDT transaction under hash
bb6767f979332d0bbd366c6445e3a57386cac1e8cc1c09607c50dc5c382a5164.

Fork 1a (Target Property 1 and 2)

Applying the Proceeds-In-First-Out (PIFO) tracing method, from there, 65,000 USDT is sent through an intermediary wallet before being split. A 30,000 USDT transaction continues through one additional wallet before being comingled with numerous other deposits. Those other USDT deposits are consolidated and sent to wallet address
TMX7iCSEuE4EZaUm13FKDwV2GUwG3ASF8M as a portion of a 1,371,782 USDT deposit. This address continued to get additional deposits and is split again into a **1,151,376 USDT** transfer to wallet **TArxGhbLdY6ApwaCYZbwdZYiHBG96heiwP (Target Property 1)** with transaction hash 0x11ce9a16b8d9596bcfbab824cc26de72d5639118890ac0ad169cdf1bef33100b; and a **619,973.34 USDT** transaction to wallet **TUNKp7upGiHt9tamt37VfjHRPUUbZ1yNKS (Target Property 2)** under transaction
0x710cd81cb45875432677453bf2c0ef758b865d0dbe53e5e91b9f7ede6dfd96f4. These wallet addresses are being used as instrumentalities to the crime of money laundering and contain proceeds directly traceable to VICTIM 1 deposits 1, 2, and 3 as well as VICTIM 2. At this point

in the layering stage of the money laundering process both Target Properties 1 and 2 were successfully frozen through cooperation with Tether Limited and is still held as of this date.

Fork 1b – (Target Property 3)

After fork 1a occurred, the remaining 21,606 USDT attributed to the Fixed Float transaction was sent as the majority of a 22,985 USDT transfer to wallet address

TVPPcD8P8QWK5eix6B6r5nVNaUFUHfUohe (Target Account 3). The remaining balance of the transaction was proceeds of a theft attributed to VICTIM 2. That deposit was commingled with existing assets in the wallet address bringing the balance to **45,834.79 USDT**. This wallet address is being used as an instrumentality to the crime of money laundering and contains proceeds directly traceable to VICTIM 1 deposits 1, 2, and 3 as well as VICTIM 2. At this point in the layering stage of the money laundering process Target Property 3 was successfully frozen through cooperation with Tether Limited and is still held as of this date.

Fork 2 (Target Property 4)

The .133 BTC originating from VICTIM 1 deposit 2 (Approx \$4,000) arrived on Tron as a portion of a 10,346.15 USDT transaction containing assets of the other suspected victims under hash 0xe79d02cf74b11afe02c4daa41f3129af11668d3751a7458daa7d6974086cfe7d. Once on the Tron network, the exact amount of 10,346 is moved to another wallet within 24 hours (due to the precise amount and proximity in time, PIFO tracing method was substituted for the matching transactions principle). There was then an 8,000 USDT transaction transferred to a wallet in the Fork 1b path where it was commingled with other assets and abandoned for the purposes of tracing. The remaining 2,346 USDT originating from the Fixed Float transaction directly traceable to VICTIM 1 deposit 2 was transferred to wallet address **TCULAeahAiC9nvurUzxvusGRLD2JxoY5Yw (Target Account 4)** as a portion of a 25,850 USDT deposit. The remaining balance of that transaction are proceeds directly traceable to VICTIM 3. These funds were then commingled with existing assets in the wallet which has a current balance of **276,966 USDT**. This wallet address is being used as an instrumentality to the crime of money laundering and contains proceeds directly traceable to VICTIM 1 deposit 2 as well as VICTIM 3. At this point in the layering stage of the money laundering process, Target Property 4 was successfully frozen through cooperation with Tether Limited and is still held as of this date.

The financial transactions involved in the above described blockchain analysis are indicative of an orchestrated attempt by a single criminal enterprise or entity to conceal the source and ownership of criminal proceeds. Despite the use of various wallet addresses and obfuscation techniques, the assets remained under the control of the criminal enterprise from the time of the initial theft and the placement of assets into the virtual asset eco system, through the layering process to the wallet addresses identified as Target Properties 1-4.

ADDITIONAL INVESTIGATION AND NOTICE OF SEIZURE

All Target Properties were restricted from movement by Tether Limited as of 4/23/24. Since that time one individual has contacted Tether Limited to claim ownership of Target Properties 1 and 2.

The claimant identified himself as Aman Kumar and contacted Tether Limited on 4/26/24 via email address [REDACTED]@myyahoo.com. Tether Limited provided Kumar with your Affiant's contact information to make claim of the assets. Additionally, your Affiant authored an email to the claimant on 5/9/2024 and again on 8/16/2024 and in each communication explained the reason for the freeze and provided the claimant with instructions to contact your affiant and/or make a claim to the assets. As of the date of this affidavit, your Affiant has not received any correspondence from the claimant. Your Affiant performed a diligent search of the provided name and email address but was not able to identify further contact information.

Your Affiant further conducted research into the IP addresses identified via business records used to transfer assets through the Fixed Float exchange. The exchange transactions for VICTIM 1 and VICTIM 2 originated from Chandigarh India and the exchange transaction for VICTIM 3 originated in Mumbai India. These facts are consistent with known organized crime rings operating from call centers within the country of India and are often carried out by numerous mules or employees working for larger organized crime elements.

Based on IP addresses obtained through the production of records by the Fixed Float Bridge, the scheme appears to have been conducted from the country of India. Your affiant used Open Source India based resources in attempt to locate records pertaining to "Iman Kumar" but was unsuccessful in identifying any individual associated with the identified email address.

Your affiant conducted a diligent analysis of the on-chain transaction activity of the wallet addresses which were target of the seizure in an attempt to identify past transactions with exposure to known entities where further records could be sought to identify the wallet owner. No exposure to known entities was located to assist in the identification of the wallet owner.

Based on the on-chain behaviors and interactions between wallets, all wallets which are target of this seizure are known to your affiant to be under the control of the same criminal entity. Based on the email received to Tether from the email address [REDACTED]@myyahoo.com, whoever maintains that email account is the possessor of all of the identified wallet addresses where target property is/was located. On May 9 2025, your affiant drafted an email to [REDACTED]@myyahoo.com which contained a Notice of Seizure document with detailed instructions on how the owner of the target property could identify themselves and make a claim to protect their assets from seizure.

Again on 5/15/25 your affiant sent a duplicate email to [REDACTED]@myyahoo.com containing the same document and details. Receipt of delivery below:

Sent: Thu 5/15/2025 9:21 PM
To: Jesse Gossman

Delivery to these recipients or groups is complete, but no delivery notification was sent by the destination server:

[REDACTED]@myyahoo.com)

Subject: Notice of Seizure

Based on the novel nature of serving legal notice via blockchain infrastructure, your affiant created five separate NFTs via a blockchain service provider which were images of the Notice of Seizure document (one for each target address and one additional as a backup). On 5/15/25 your affiant sent each of the wallets containing the target property an independent NFT of the Notice of Seizure. The delivery of each NFT is recorded on the blockchain as indicated below.



CASE #: 34-2312-235579 / CY-73-0007

TO: human@twinkl.co.uk

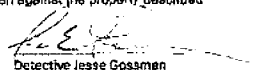
Private Key Holder of Iron Wallet Address **TC1H AaaaBAC9pxuU1z99u8B1Q21x9Y5Y**

2025-05-08 15:24:21 (UTC) received 2,037,288.498336 USDT (Tether)

YOU HAVE THE RIGHT to request an adversarial preliminary hearing to have a court determine whether probable cause exists to believe the property seized has been or is being used in violation of the Florida Contraband Forfeiture Act. The request must be made within fifteen (15) days of the receipt of this notice.

IN ORDER TO REQUEST such a hearing, you must make the request in writing, by Certified Mail, Return Receipt Requested, to the Office of the Attorney General, Cyber Fraud Enforcement Unit, 3507 E Frontage Rd #200, Tampa, FL 33607. You must provide a copy of this Notice with your request. You must also provide your address so you can be notified of the time, date, and place of the hearing.

PLEASE NOTE THAT the post-seizure adversarial hearing is not mandatory and you need not request a hearing to later contest the action taken against the property described herein.



Jesse Gershwin, CBE

[illegible]

Revista de la Facultad de Ciencias Exactas y Naturales, Vol. 19, No. 1, 1970

TC74

[illegible]

The NFT holders are listed below as publicly viewable on any publicly viewable blockchain explorer.

| # | Holders | Amount | Percentage | Latest Txn Time (UTC) |
|---|---------|--------|------------|-----------------------|
| 1 | | 1 | 20.00% | 2025-05-15 01:55:04 |
| 2 | | 1 | 20.00% | 2025-05-15 01:55:04 |
| 3 | | 1 | 20.00% | 2025-05-15 01:55:04 |
| 4 | | 1 | 20.00% | 2025-05-15 01:55:04 |
| 5 | | 1 | 20.00% | 2025-05-15 01:55:04 |

Based on the above facts and circumstances, your Affiant finds probable cause exists that the above-mentioned property was used as an instrumentality to commit a felony and therefore in violation of the Florida Contraband Forfeiture Act (FCFA) Florida Statutes §§ 932.701-932.704. As such, your Affiant has made a diligent effort to identify and provide a Notice of Seizure to an as yet unidentified USDT user(s) possessing the private keys to Tron Network Wallet Addresses **TArxGhbLdY6ApwaCYZbwdZYiHBG96heiwp** (Target Property #1), **TUNKp7upGiHt9tamt37VfjHRPUUbZ1yNKS** (Target Property #2), **TVPPcD8P8QWK5eix6B6r5nVNaUFUHfUohe** (Target Property #3), and **TCULAeahAiC9nvurUzxvusGRLD2JxoY5Yw** (Target Property #4).


Despite your affiant's diligent efforts to locate and notify the owner of the seized property, the owner of the above listed wallet addresses has likewise made a diligent effort to conceal their identity and obfuscate their connection to the illicit proceeds contained within the target wallets.

WHEREFORE, based upon the facts outlined above, your affiant submits this sworn affidavit in compliance with Florida law.



AFFIANT/DETECTIVE JESSE GOSSMAN
FORT LAUDERDALE POLICE DEPARTMENT

The foregoing instrument was duly sworn to and subscribed before me this 16 day of May, 2025, by Detective Jesse Gossman who is personally known to me or who has produced (ID) as identification and who DID take an oath.

Officer Administering the Oath (Signature) 

Officer Administering the Oath (Printed Name) Espinal Burgos 2063

EXHIBIT B



NOTICE OF SEIZURE

DATE: May 9, 2025

CASE #: 34-2312-235579 / CY-73-0007

TO: [REDACTED]kumar@myyahoo.com

Private Key Holder of Tron Wallet Address **TArxGhbLdY6ApwaCYZbwdZYiHBG96heiwp**

Private Key Holder of Tron Wallet Address **TUNKp7upGiHt9tamt37VfjHRPUUbZ1yNKS**

Private Key Holder of Tron Wallet Address **TVPPcD8P8QWK5eix6B6r5nVNaUFUHfUohe**

Private Key Holder of Tron Wallet Address **TCULAeahAiC9nvurUzxvusGRLD2JxoY5Y**

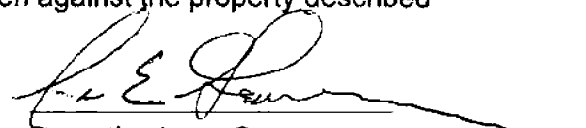
THIS IS TO ADVISE you that on May 8, 2025, the Fort Lauderdale Police Department received confirmation of seizure of the following units of the listed cryptocurrencies from the identified wallet addresses for a violation of the Florida Contraband Forfeiture Act, Sections 932.701-7062, Florida Statutes:

2025-05-08 15:24:21 (UTC) received 2,037,288.496339 USDT (Tether)

YOU HAVE THE RIGHT to request an adversarial preliminary hearing to have a court determine whether probable cause exists to believe the property seized has been or is being used in violation of the Florida Contraband Forfeiture Act. The request must be made within fifteen (15) days of the receipt of this notice.

IN ORDER TO REQUEST such a hearing, you must make the request in writing, by Certified Mail, Return Receipt Requested, to the Office of the Attorney General, Cyber Fraud Enforcement Unit, 3507 E Frontage Rd #200, Tampa, FL 33607. You must provide a copy of this Notice with your request. You must also provide your address so you can be notified of the time, date, and place of the hearing.

PLEASE NOTE THAT the post-seizure adversarial hearing is not mandatory and you need not request a hearing to later contest the action taken against the property described herein.


Detective Jesse Gossman

- ☐ Mailed by Registered Mail
- ☒ Sent via Email
- ☐ Hand Delivered, Accepted by

Police Department

1300 West Broward Boulevard, Fort Lauderdale, Florida 33312

Telephone (954) 828-5700, Fax (954) 828-6001

www.fortlauderdale.gov

