

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

UNDER SEAL

In the Matter of the Seizure of:

Case Number:

THE FUNDS ON DEPOSIT WITH TETHER at the following addresses:
0x1bdd6956015976209e34e5f47C574A0f2cA9BD87 (SUBJECT ASSET #1),
0x7c214b43350B51B8C2B72c0C2b10b764Fc9774c6 (SUBJECT ASSET #2),
0xcf95f287E2856c34130B9D31859f3b2C29b45d50 (SUBJECT ASSET #3),
0xB8C348f248AD0493Ae2e6640D30ce3986413Af23 (SUBJECT ASSET #4), and
0x9404a2CBD5e46B91e814909c49fa071F31C86b7d (SUBJECT ASSET #5),
further Described in Attachment A.

APPLICATION AND AFFIDAVIT FOR A SEIZURE WARRANT

I, a federal law enforcement officer or attorney for the government, request a seizure warrant and state under penalty of perjury that I have reason to believe that the following property is subject to forfeiture to the United States of America under 18 U.S.C. § 981, 18 U.S.C. § 982, 21 U.S.C. § 853, and 28 U.S.C. § 2461:

funds on deposit with Tether at the following addresses:

0x1bdd6956015976209e34e5f47C574A0f2cA9BD87 (SUBJECT ASSET #1),
0x7c214b43350B51B8C2B72c0C2b10b764Fc9774c6 (SUBJECT ASSET #2),
0xcf95f287E2856c34130B9D31859f3b2C29b45d50 (SUBJECT ASSET #3),
0xB8C348f248AD0493Ae2e6640D30ce3986413Af23 (SUBJECT ASSET #4), and
0x9404a2CBD5e46B91e814909c49fa071F31C86b7d (SUBJECT ASSET #5).

The application is based on these facts:

See Attached Affidavit,

Continued on the attached sheet.



Applicant's Signature

JAYNA KADEL, Special Agent
Federal Bureau of Investigation

Printed name and title

Pursuant to Fed. R. Crim. P. 4.1, this Application is presented by reliable electronic means. The above-named agent provided a sworn statement attesting to the truth of the statements in the Application and Affidavit by telephone.

Date:

Judge's signature

M. David Weisman, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT OF SPECIAL AGENT JAYNA KADEL

Jayna Kadel, Special Agent, Federal Bureau of Investigation, being duly sworn, deposes and says:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent of the Federal Bureau of Investigation. I have been so employed since approximately 2014.

2. As part of my duties as an FBI Special Agent, I investigate criminal violations relating to white collar crime, including mail, wire, and bank fraud. In addition, I have received training on how people use computers to commit crimes and the law enforcement techniques that can be used to investigate and disrupt such activity. I have participated in federal search and seizure warrants to include warrants pertaining to the seizure of digital information and digital assets.

3. This affidavit is based upon my personal knowledge, interviews of witnesses, my review of documents and other evidence, my conversations with other law enforcement personnel to include forensic accountants knowledgeable about cryptocurrency, information received concerning the use of computers in criminal activity, and my training and experience. Because this affidavit, and attached exhibits, are being submitted for the limited purpose of establishing probable cause, they do not include all the facts that I have learned during my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

PURPOSE OF AFFIDAVIT

4. This affidavit is submitted in support of an application for a combined criminal and civil forfeiture seizure warrant for the following assets: the equivalent value of USDT as currently associated with the following addresses: 0x1bdd6956015976209e34e5f47C574A0f2cA9BD87 (**SUBJECT ASSET #1**), 0x7c214b43350B51B8C2B72c0C2b10b764Fc9774c6 (**SUBJECT ASSET #2**), 0xcf95f287E2856c34130B9D31859f3b2C29b45d50 (**SUBJECT ASSET #3**), 0xB8C348f248AD0493Ae2e6640D30ce3986413Af23 (**SUBJECT ASSET #4**), and 0x9404a2CBD5e46B91e814909c49fa071F31C86b7d (**SUBJECT ASSET #5**). Throughout this affidavit, I will refer to these addresses collectively as the “**SUBJECT ASSETS**.”

5. On January 25, 2024, the government submitted an application to seize these same **SUBJECT ASSETS** to this Court in case number 24 M 43. That same day, this Court signed a seizure warrant in case number 24 M 43 for the **SUBJECT ASSETS**. The January 25, 2024 application is attached as Exhibit 1 and is incorporated into this affidavit. The January 25, 2024 seizure warrant is attached as Exhibit 2.

6. As explained in Exhibit 1, Tether Limited (“Tether”) is the company that manages the smart contracts and treasury (i.e., reserve assets) for USDT. After obtaining the seizure warrant on January 25, 2024, the government was unable to serve Tether with the seizure warrant within the allotted 14 days. More specifically, according to an FBI agent in contact with Tether, Tether is located in the British Virgin Islands, and the company is willing to accept and execute this seizure warrant by “burning” or destroying the addresses that comprise the **SUBJECT ASSETS** (and by extension the USDT tokens associated with them). Then, Tether would reissue the equivalent amount of USDT tokens associated with each address and transfer that USDT to a government-controlled wallet. However, this process requires coordination between law

enforcement and Tether in order to execute the seizure warrant and provide the **SUBJECT ASSETS** to law enforcement. This coordination took longer than anticipated. As a result, your affiant now seeks another seizure warrant for the **SUBJECT ASSETS**.

7. As set forth in Exhibit 1, I submit that there is probable cause to believe that the **SUBJECT ASSETS** constitute proceeds, or property traceable to proceeds, of a wire fraud offense or offenses committed in violation of 18 U.S.C. § 1343 and were involved in the commission of a money laundering offense or offenses committed in violation of 18 U.S.C. § 1956 (collectively, hereafter, the “**SUBJECT OFFENSES**”). The **SUBJECT ASSETS** are, therefore, subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(A) and (a)(1)(C) (civil forfeiture on money laundering and proceeds theories) and 18 U.S.C. §§ 982(a)(1) and 982(b)(1) and 28 U.S.C. § 2461 (criminal forfeiture on money laundering and proceeds theories).

CONCLUSION

8. I respectfully submit that Exhibit 1 presents probable cause to believe that the private wallets with addresses **0x1bdd69**, **0x7c214b**, **0xcf95f2**, **0xB8C348**, and **0x9404a2** received proceeds of the above-described fraud scheme perpetrated against Victim A, Victim B, Victim C, Victim D, and Victim E and, further, were used to commit concealment money laundering transactions in violation of 18 U.S.C. §§ 1956 (a)(1)(B)(i), (a)(2)(A), (a)(2)(B)(i), and (h) and the **SUBJECT ASSETS** are property involved in the underlying fraud. On that basis, I seek authority to obtain seizure warrants for the **SUBJECT ASSETS**.

A large, stylized handwritten signature in black ink, reading "Jayna Kadel". The signature is written over a horizontal line.

Applicant's Signature

JAYNA KADEL, Special Agent,
Federal Bureau of Investigation

Pursuant to Fed. R. Crim. P. 4.1, this Application is presented by reliable electronic means. The above-named agent provided a sworn statement attesting to the truth of the statements in the Application and Affidavit by telephone.

Date:

Judge's signature

M. David Weisman, U.S. 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 addresses referenced below. Tether shall effectuate this process by (1) burning the USDT tokens currently associated with the virtual currency addresses referenced below and (2) reissuing the equivalent value of USDT tokens to a U.S. law enforcement-controlled virtual currency account. Tether shall provide reasonable assistance in implementing the terms of this seizure warrant and take no unreasonable action to frustrate its implementation.

0x1bdd6956015976209e34e5f47C574A0f2cA9BD87 (SUBJECT ASSET #1),

0x7c214b43350B51B8C2B72c0C2b10b764Fc9774c6 (SUBJECT ASSET #2),

0xcf95f287E2856c34130B9D31859f3b2C29b45d50 (SUBJECT ASSET #3),

0xB8C348f248AD0493Ae2e6640D30ce3986413Af23 (SUBJECT ASSET #4), and

0x9404a2CBD5e46B91e814909c49fa071F31C86b7d (SUBJECT ASSET #5).

Exhibit 1

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

Case Number: 24 M 43

In the Matter of the Seizure of:

THE FUNDS ON DEPOSIT WITH TETHER at the following addresses:
0x1bdd6956015976209e34e5f47C574A0f2cA9BD87 (SUBJECT ASSET #1),
0x7c214b43350B51B8C2B72c0C2b10b764Fc9774c6 (SUBJECT ASSET #2),
0xcf95f287E2856c34130B9D31859f3b2C29b45d50 (SUBJECT ASSET #3),
0xB8C348f248AD0493Ae2e6640D30ce3986413Af23 (SUBJECT ASSET #4), and
0x9404a2CBD5e46B91e814909c49fa071F31C86b7d (SUBJECT ASSET #5),
further Described in Attachment A.

APPLICATION AND AFFIDAVIT FOR A SEIZURE WARRANT

I, a federal law enforcement officer or attorney for the government, request a seizure warrant and state under penalty of perjury that I have reason to believe that the following property is subject to forfeiture to the United States of America under 18 U.S.C. § 981, 18 U.S.C. § 982, 21 U.S.C. § 853, and 28 U.S.C. § 2461:

funds on deposit with Tether at the following addresses:

0x1bdd6956015976209e34e5f47C574A0f2cA9BD87 (SUBJECT ASSET #1),
0x7c214b43350B51B8C2B72c0C2b10b764Fc9774c6 (SUBJECT ASSET #2),
0xcf95f287E2856c34130B9D31859f3b2C29b45d50 (SUBJECT ASSET #3),
0xB8C348f248AD0493Ae2e6640D30ce3986413Af23 (SUBJECT ASSET #4), and
0x9404a2CBD5e46B91e814909c49fa071F31C86b7d (SUBJECT ASSET #5).

The application is based on these facts:

See Attached Affidavit,

Continued on the attached sheet.



Applicant's Signature

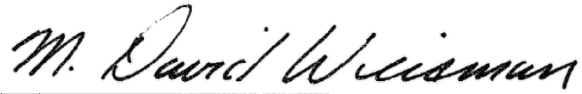
JAYNA KADEL, Special Agent
Federal Bureau of Investigation

Printed name and title

Pursuant to Fed. R. Crim. P. 4.1, this Application is presented by reliable electronic means. The above-named agent provided a sworn statement attesting to the truth of the statements in the Application and Affidavit by telephone.

Date:

January 25, 2024



Judge's signature

M. David Weisman, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT OF SPECIAL AGENT JAYNA KADEL

Jayna Kadel, Special Agent, Federal Bureau of Investigation, being duly sworn, deposes and says:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent of the Federal Bureau of Investigation. I have been so employed since approximately 2014.

2. As part of my duties as an FBI Special Agent, I investigate criminal violations relating to white collar crime, including mail, wire, and bank fraud. In addition, I have received training on how people use computers to commit crimes and the law enforcement techniques that can be used to investigate and disrupt such activity. I have participated in federal search and seizure warrants to include warrants pertaining to the seizure of digital information and digital assets.

3. This affidavit is based upon my personal knowledge, interviews of witnesses, my review of documents and other evidence, my conversations with other law enforcement personnel to include forensic accountants knowledgeable about cryptocurrency, information received concerning the use of computers in criminal activity, and my training and experience. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

PURPOSE OF AFFIDAVIT

4. This affidavit is submitted in support of an application for a combined criminal and civil forfeiture seizure warrant for the following assets: the equivalent value of USDT as currently

associated with the following addresses: 0x1bdd6956015976209e34e5f47C574A0f2cA9BD87 (SUBJECT ASSET #1), 0x7c214b43350B51B8C2B72c0C2b10b764Fc9774c6 (SUBJECT ASSET #2), 0xcf95f287E2856c34130B9D31859f3b2C29b45d50 (SUBJECT ASSET #3), 0xB8C348f248AD0493Ae2e6640D30ce3986413Af23 (SUBJECT ASSET #4), and 0x9404a2CBD5e46B91e814909c49fa071F31C86b7d (SUBJECT ASSET #5). Throughout this affidavit, I will refer to these addresses collectively as the “SUBJECT ASSETS.”

5. As set forth below, I submit that there is probable cause to believe that the SUBJECT ASSETS constitute proceeds, or property traceable to proceeds, of a wire fraud offense or offenses committed in violation of 18 U.S.C. § 1343 and were involved in the commission of a money laundering offense or offenses committed in violation of 18 U.S.C. § 1956 (collectively, hereafter, the “SUBJECT OFFENSES”). The SUBJECT ASSETS are, therefore, subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(A) and (a)(1)(C) (civil forfeiture on money laundering and proceeds theories) and 18 U.S.C. §§ 982(a)(1) and 982(b)(1) and 28 U.S.C. § 2461 (criminal forfeiture on money laundering and proceeds theories).

FORFEITURE AND SEIZURE AUTHORITY

6. As to civil forfeiture, under 18 U.S.C. § 981(a)(1)(A), “[a]ny property, real or personal, involved in a transaction in violation of [18 U.S.C. § 1956], or any property traceable to such property,” is subject to civil forfeiture to the United States. In addition, under 18 U.S.C. § 981(a)(1)(C), with cross references to 18 U.S.C. §§ 1956(c)(7) and 1961(1), “[a]ny property, real or personal, which constitutes or is derived from proceeds traceable to a violation of” fraud are subject to civil forfeiture to the United States. In turn, property subject to civil forfeiture under 18 U.S.C. § 981(a) may be seized pursuant to 18 U.S.C. § 981(b).

7. As to criminal forfeiture, under 18 U.S.C. § 982(a)(1), “[t]he court, in imposing sentence on a person convicted of an offense in violation of [18 U.S.C. § 1956] shall order that the

person forfeit to the United States any property, real or personal, involved in such offense, or any property traceable to such property.” As property subject to criminal forfeiture under 18 U.S.C. § 982(a)(1), the SUBJECT ASSETS may be seized pursuant to 21 U.S.C. § 853(f) (by 18 U.S.C. § 982(b)(1)).

8. Based on the facts and circumstances set forth below, I submit that there exists probable cause to believe that the funds held in the SUBJECT ASSETS are:

- a. Funds traceable to, and are therefore proceeds of, wire fraud, committed in violation of 18 U.S.C. § 1343, and therefore are subject to civil forfeiture under 18 U.S.C. § 981(a)(1)(C), including cross-references to 18 U.S.C. §§ 1956(c)(7) and 1961(1), and subject to criminal forfeiture under 28 U.S.C. § 2461(c); and
- b. Funds involved in or traceable to money laundering offenses, committed in violation of 18 U.S.C. § 1956, and therefore are subject to civil forfeiture under 18 U.S.C. § 981(a)(1)(A), and subject to criminal forfeiture under 18 U.S.C. § 982(a)(1).

9. With respect to seizure, 21 U.S.C. § 853(f) specifically provides that a court may issue a criminal seizure warrant when it “determines that there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture and that an order under [21 U.S.C. § 853(e)] may not be sufficient to assure the availability of the property for forfeiture.” As set forth further below, there is a substantial risk that the SUBJECT ASSETS will be withdrawn, moved, dissipated, or otherwise become unavailable for forfeiture unless immediate steps are taken to secure them at the time the requested searches are executed. As a form of cryptocurrency, some of the SUBJECT ASSETS are inherently portable. I therefore submit that a

protective order under 21 U.S.C. § 853(e) would not be sufficient to assure that the SUBJECT ASSETS will remain available for forfeiture.

10. Thus, to seize the SUBJECT ASSETS in this case for criminal or civil forfeiture, the Government must show that there is probable cause to believe that underlying wire fraud or subsequent money laundering conduct occurred, and that the SUBJECT ASSETS have a nexus to that offense—namely, that the SUBJECT ASSETS constitute wire fraud proceeds or property traceable to such proceeds, were involved in money laundering or are traceable to property involved in money laundering, or both. *See* 18 U.S.C. §§ 981(a)(1)(A), (a)(1)(C), 982(a)(1), and (b)(1), and 28 U.S.C. § 2461.

11. As set forth below, the SUBJECT ASSETS include cryptocurrency amounts that both (a) are traceable to proceeds of a wire fraud scheme involving financial fraud and (b) were transferred in relatively small batches of currency through a series of intermediary addresses for no discernable purpose, very probably in an effort to launder the proceeds through the listed addresses as part of concealment money laundering conduct. All the SUBJECT ASSETS are therefore subject to forfeiture because they were involved in apparent concealment money laundering conduct. *See, e.g., United States v. Guerrero*, 2021 WL 2550154, *9 (N.D. Ill. June 22, 2021) (money that was commingled with fraud proceeds facilitated the concealment laundering of the fraud proceeds and, accordingly, property acquired with the commingled funds was forfeitable as property traceable to property involved in a money laundering offense); *United States v. Romano*, 2021 WL 1711633, *5-6 (E.D.N.Y. Apr. 29, 2021) (by laundering fraud proceeds through their accounts, to commingle the proceeds with other funds for a concealment laundering purpose, the defendants made the commingled funds forfeitable as facilitating property).

12. For the reasons listed above, the United States seeks combined criminal and civil seizure warrants, authorizing law enforcement to seize the SUBJECT ASSETS and preserve them pending further forfeiture proceedings.

BACKGROUND ON CRYPTOCURRENCY

13. Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions:

a. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to-peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are Bitcoin, Litecoin, and Ether. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a “blockchain,” which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.¹ Cryptocurrency, itself, is not illegal in the United States.

¹ Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

b. Bitcoin² (“BTC”) is a type of cryptocurrency. Payments or transfers of value made with bitcoin are recorded in the Bitcoin blockchain and thus are not maintained by any single administrator or entity. As mentioned above, individuals can acquire bitcoin through exchanges (i.e., online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), bitcoin ATMs, or directly from other people.

c. Ether (“ETH”) is a cryptocurrency that is open source, public, has a blockchain, and is distributed on a platform that uses “smart contract” technology. The public ledger is the digital trail of the Ethereum blockchain, which allows anyone to track the movement of ETH. Smart contracts allow developers to create markets, store registries of debts, and move funds in accordance with the instructions provided in the contract's code, without any type of middleman or counterparty controlling a desired or politically motivated outcome, all while using the Ethereum blockchain protocol to maintain transparency. Smart contract technology is one of Ethereum's distinguishing characteristics and an important tool for companies or individuals executing trades on the Ethereum blockchain. When engaged, smart contracts automatically execute according to the terms of the contract written into lines of code. A transaction contemplated by a smart contract occurs on the Ethereum blockchain and is both trackable and irreversible.

d. Tether (“USDT”) and USDC are alternative types of cryptocurrency or altcoin tokens. Payments or transfers of value made with USDT and USDC are recorded

² Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use “Bitcoin” (singular with an uppercase letter B) to label the protocol, software, and community, and “bitcoin” (with a lowercase letter b) to label units of the cryptocurrency. That practice is adopted here.

on whichever blockchain network they exist, but unlike decentralized cryptocurrencies like BTC, USDT has some anatomical features of centralization. One centralized feature is that USDT and USDC are “stablecoins,” where the value of the digital asset is pegged to a reference asset (in this case, the US dollar); for each USDT and USDC issued, the tokens are represented to be backed by \$1 of asset reserves. These characteristics make them theoretically less volatile than BTC, and consequently wallet holders often hedge their cryptocurrency holdings into USDT in an attempt to protect their receipt or earnings value, so it is not affected by the rest of the cryptocurrency market.

e. Tether Limited (“Tether”) is the company that manages the smart contracts and treasury (*i.e.*, reserve assets) for USDT. Circle Internet Financial, LCC (“Circle”) is the company that manages the smart contracts and treasury for USDC. Because Tether and Circle manage the smart contracts for USDT and USDC (respectively), they are able to blacklist some addresses containing USDT and USDC. For example, as is relevant to this application, Tether is able to blacklist addresses on the Ethereum network, rendering them inaccessible to whomever controls the private keys to the blacklisted addresses. In the instant case, at the request of law enforcement, Tether acted to freeze/blacklist the USDT associated with the SUBJECT ASSETS and has indicated that they will continue to do so until they receive the instant warrant.

f. Individuals can also acquire cryptocurrencies by “mining.” An individual can “mine” bitcoins by using his or her computing power to solve a complicated algorithm and verify and record payments on the blockchain. Individuals are rewarded for this task by receiving newly created units of a cryptocurrency. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop

computers and smart phones. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are therefore sometimes described as “pseudonymous,” meaning that they are partially anonymous. And while it’s not completely anonymous, bitcoin allows users to transfer funds more anonymously than would be possible through traditional banking and financial systems.

g. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or “public key”) and the private address (or “private key”). A public address is usually represented as a case-sensitive string of letters and numbers, 26–90 characters long, often depending on the cryptocurrency protocol. Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an address’s private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

h. Although cryptocurrencies such as bitcoin and Ether have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes—for example, as payment for illegal goods and services and to commit money laundering. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement’s efforts to track purchases. The value of cryptocurrency is generally much more volatile than that of fiat currencies. As of January 15, 2024, one BTC is worth approximately \$42,499.34, one ETH is worth approximately \$2,510.63, and one USDT is worth approximately \$.999723.³

i. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device (“hardware wallet”), downloaded on a PC or laptop (“desktop wallet”), with an Internet-based cloud storage provider (“online wallet”), as a mobile application on a smartphone or tablet (“mobile wallet”), printed public and private keys (“paper wallet”), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can access the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g. Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code⁴ with the public and private key embedded in the code. Paper wallet keys are not

³ Historical data as reported by Yahoo Finance.

⁴ A QR code is a matrix barcode that is a machine-readable optical label.

stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a “recovery seed” (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase).

j. “Exchangers” and “exchanges” are individuals or companies that exchange bitcoin or other cryptocurrencies for other currencies, including U.S. dollars. According to the United States Department of Treasury, Financial Crimes Enforcement Network (“FinCEN”) Guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses.⁵ Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). From my training and experience, I know that registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering (“AML”) regulations, “Know Your Customer” (“KYC”) protocols, and other verification procedures similar to those employed by traditional financial institutions. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and the full bank account and routing numbers that the customer links to an exchange account. As a result, there is significant market demand for illicit cryptocurrency-for-fiat-currency exchangers, who lack AML or KYC protocols and often also advertise their ability to offer customers anonymity. These illicit exchangers routinely exchange fiat currency for cryptocurrencies

⁵ See “Application of FinCEN’s Regulations to Person Administering, Exchanging, or Using Virtual Currencies,” *available at* <https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering>.

by meeting customers in person or by shipping cash through the mail. Due to the illicit nature of these transactions and their customers' desire for anonymity, such exchangers are frequently able to charge a higher exchange fee, often as high as 9–10% (in contrast to registered and Bank Secrecy Act-compliant exchangers, who may charge fees as low as 1–2%).

k. Some companies offer cryptocurrency wallet services, which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the specific device on which the wallet application was installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet as described above, law enforcement may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet. As referenced above, in this matter, the SUBJECT ASSETS are associated with virtual currency addresses that exist on the Ethereum network. Should this application be granted,

the accompanying warrant would be transmitted to Tether, at which time Tether would “burn” or destroy the addresses that comprise the SUBJECT ASSETS (and by extension the USDT tokens associated with them). Tether would then reissue the equivalent amount of USDT tokens associated with each address and transfer that USDT to a government-controlled wallet.

FACTUAL BACKGROUND

14. In summary, the FBI is investigating a fraud scheme wherein the perpetrators pose as employees of Microsoft or Apple and the victim’s bank to convince the victim that they are the subject of a hacking incident. The scheme is initiated via a computer dialogue box (or “popup”) that indicates the victim’s computer is compromised and directs the victim to call Microsoft or Apple for assistance. Typically, the perpetrators convince the victim his/her financial accounts are at risk and that he/she needs to move money from traditional bank accounts to cryptocurrency to keep it safe from the hackers. Once the victim’s money is converted to cryptocurrency, the perpetrators arrange for cryptocurrency to be transferred to digital currency wallets the victim does not control and are presumably controlled by the perpetrators and their co-conspirators. The scheme has affected individuals located all over the United States including at least two known victims located in the Northern District of Illinois.

15. In support of the investigation, the FBI was conducting analysis of the currency transfers into an address that received proceeds from a victim located in Evanston, Illinois,⁶ address 0x16A69fe4fFCA1Bc32A0EF15F5Ff9629DA313BAa1 (hereinafter **0x16A69f**). The

⁶ Based on interviews with the victim in Evanston, the victim lost between \$2 to \$3 million in a scheme similar to the one described in this affidavit.

FBI conducted reverse blockchain analysis⁷ in an attempt to identify the source of the other funds stored in 0x16A69f. During this process, the FBI identified several intermediary private addresses which had also transferred funds into 0x16A69f. Some of those intermediary addresses received funds from addresses traced to crypto exchange Crypto.com. One such private address was 0x3fa26E5539dfef7b4750b26565CFCd60E8556d28 (hereinafter **0x3fa26E**).⁸ Through legal process, the FBI obtained subscriber account information from Crypto.com. The subscriber records identified the account holder as a resident of New Jersey, hereinafter referred to as Victim A.

16. Between March 20 and March 23, 2023, law enforcement conducted several interviews of Victim A. Victim A stated in November 2022, he was working on his computing device when he received a popup alert directing him to contact Apple. Victim A called the number provided and spoke to an individual claiming to work for Apple, and later to an individual claiming to work in the fraud department of Victim A's bank (these unidentified individuals are hereinafter referred to as the "scammers"). The scammers convinced Victim A his Social Security Number (SSN) was compromised, loans had been attempted using Victim A's name and SSN, and his financial assets were at risk. The scammers convinced Victim A he needed to take steps to secure his assets. The scammers suggested they use a secure "treasury account" which was purportedly completely independent of Victim A's compromised SSN and would protect his funds until a new SSN was issued. Part of the process of transferring funds to this account involved the use of cryptocurrency, which the scammers suggested further separated Victim A's funds from his at-

⁷ "Reverse blockchain analysis" is a term utilized by your affiant to describe the process by which deposits into an address are traced backwards through the blockchain to identify the original source of funds.

⁸ As discussed later, this is the address of Victim A's Exodus wallet.

risk SSN. The scammers said the process was safe and arranged by his bank and that all funds would be returned to his original accounts at some later date.

17. According to Victim A, the scammers provided Victim A with a letter purportedly from the United States Federal Reserve, bearing the signature of Jerome Powell. The letter states, in part, that Victim A is “under contract with the Federal Reserve of United States for IDENTITY THEFT with Mr. Kevin Lawson assigned as fraud prevention officer for completing the Re-validation of your bank accounts and financial assets.”⁹ Law enforcement shared an image of this letter with a contact at the United States Federal Reserve Board, Office of Inspector General, who indicated the letter is not authentic. According to Victim A, the scammers also provided Victim A with a letter purportedly from the bank where Victim A maintained his individual retirement account. The letter states in part, “In regards to the ongoing Identification Theft & Financial Fraud case of [Victim A], Merrill Fraud Prevention department has decided that majority of the funds from his respective Merrill accounts will be liquidated and transferred to his Secure Treasury Account” and “once all his Merrill accounts are completely secured, entire funds will be transferred back at the completion of the case.” The letter further states the case is “being investigated by Mr. Kevin Lawson...under the supervision of Federal Trade Commission & Social Security Administration.” Based on my training and experience, it would be highly irregular for a government agency to task the investigation of a fraud case to a civilian, non-governmental official.

⁹ “Kevin Lawson” is the name provided by the individual claiming to work for Victim A’s bank. This name was provided to several other victims known to your Affiant, who also lost money in a similar manner to Victim A. In each case, Lawson purported to work for the victim’s financial institution – in one instance, PNC Bank, in another instance, USAA Bank.

18. According to Victim A, the scammers requested Victim A install a software program on his devices which allows a third-party remote access to a computer. Victim A indicated there were times when he could see someone “monitoring” his computer; for example, he could see someone remotely moving the cursor. The scammers also had Victim A leave a phone line “open” during the day so they could monitor activity. Victim A stated he would alternate between his cellular telephone and home phone number, in two-to-four-hour increments.¹⁰ The scammers communicated with Victim A through what they described as a “secure line” hosted by Apple.¹¹

19. According to Victim A, the scammers provided instructions to Victim A on how to make the money transfers. The scammers directed Victim A go to a local bank branch and initiate wire transfers to PeopleFirst Bank and Metropolitan Community Bank. The scammers told Victim A these banks had agreements with Crypto.com. The scammers provided details like bank address, account or routing number, and a reference or unique code. The scammers told Victim A they did not know who compromised his SSN so he needed to leave his cell phone on while visiting the branch so they (the scammers) could monitor for indicators of fraudulent behavior by the branch employees. The scammers assisted Victim A in setting up an account with Crypto.com, which included taking a photograph of himself sitting at his computer. The scammers directed Victim A

¹⁰ According to Victim A, he was in telephone contact with the scammers from approximately 9:00 AM or 9:30 AM until 4:00 PM or 5:00 PM each day.

¹¹ The secure line, 425-588-0278, is assigned to a voice over IP telephone service. The subscriber records indicate the subscriber is “kush0895”, not Apple. IP logs indicate the account was registered from an IP address in the Punjab state of India. This same VOIP telephone number was also provided to the FBI by the Evanston, Illinois victim, as one of the telephone numbers the scammers utilized.

to install Exodus, a digital currency wallet,¹² on his devices. Approximately 24 hours after sending the wire transfer, Victim A received an email from Crypto.com indicating the funds were available. The scammers then provided Victim A step-by-step instructions, via telephone, on how to make transfers, which included the use of the Crypto.com account to make transfers from Victim A's U.S. currency to cryptocurrency that, according to the scammers, would ultimately be deposited into the treasury accounts. The scammers told Victim A he had two treasury accounts: one for the funds that originated from his checking account and one for the funds that originated from his individual retirement account. The scammers provided Victim A with documents entitled "confirmation letter" on bank letterhead which purport to show deposits into these treasury accounts. Victim A stated these confirmations reassured him everything was legitimate and is part of the reason he continued to engage with the scammers.

20. During an interview with Victim A, Victim A stated he followed the same procedures on behalf of funds belonging to his wife, Victim B.

21. During an interview with Victim A, Victim A stated he transferred between \$3 and \$4 million at the direction of the scammers. As described below, Victim A's statement related to these transfers is corroborated by financial records obtained in the investigation.

22. According to publicly available information, Crypto.com is the "world's leading cryptocurrency platform" where users can "buy Bitcoin, Ethereum, and 250+ cryptocurrencies" and "trade with 20+ fiat currencies."¹³ At the direction of the scammers, Victim A caused the following wire transfers to be sent from his traditional bank account held by a bank headquartered

¹² Exodus wallet is a "self-custody" or non-custodial wallet, meaning the user of the wallet is acting as his/her own custodian of digital currency deposited in that wallet. The user accesses his/her wallet with a secret recovery phrase known as a seed phrase or a PIN code.

¹³ From <https://crypto.com>, last checked January 10, 2024.

in Cherry Hill, New Jersey, to the Crypto.com correspondent bank (Metropolitan Commercial Bank) headquartered in New York:¹⁴

Date	Transfer Amount	Credit to Account
11/30/2022	\$495,000.00	Victim A
12/08/2022	\$495,000.00	Victim B
01/09/2023	\$320,237.36	Victim A
03/09/2023 ¹⁵	\$535,000.00	Victim A
03/17/2023 ¹⁶	\$530,000.00	Victim B

23. The FBI, through legal process, obtained account records from Crypto.com for an account owned by Victim A and an account owned by Victim B¹⁷ and account records from Athena Bitcoin for an account owned by Victim A.¹⁸ Victim A provided the FBI with a Microsoft Excel

¹⁴ Based on my training and experience, bank wire transfers usually require the use of one or more interstate wire communications because the parties to the transaction, including the originator (in this case, the Victims), the originator's bank, the beneficiary bank, the beneficiary, and the processor—often the Federal Reserve Banks's Fedwire system—are typically geographically dispersed. In this case, the Victim was located in New Jersey, his bank was headquartered in New Jersey, and the receiving bank was located in New York. I know from experience that Fedwire data centers are located in New Jersey and Texas, and transfers are processed in a multi-step process. As such, it is reasonable to believe some portion of the Victim's wire transfers affected interstate commerce and traveled interstate.

¹⁵ This transfer was debited from Victim A's bank account on March 8, 2023 and posted to his Crypto.com account March 9, 2023.

¹⁶ This transfer was debited from Victim A's bank account on March 16, 2023 and posted to his Crypto.com account March 17, 2023.

¹⁷ Victim A stated both he and his wife opened accounts at Crypto.com at the direction of the scammers. Victim A stated he made all of the transfers on behalf of Victim B.

¹⁸ According to publicly available information, Athena Bitcoin "is focused on developing, owning, and operating a global network of Athena-branded Bitcoin ATM machines" and "operates an over-the-counter ("OTC") desk known as ACE (Athena Crypto Exchange) for private clients and trade customers." From <https://athenabitcoin.com/the-company/>, last assessed January 10, 2024. According to Victim A, he transferred money to Athena Bitcoin at the direction of the scammers. Financial records obtained in the investigation corroborate Victim A's statement and indicate approximately \$1,600,000 was transferred to Victim A's Athena Bitcoin account.

transaction history from his Exodus wallet which consists of both a Tether (USDT) address, **0x3fa26E**, and a Bitcoin address **bc1qth95kp3d39rpytnu9dpluh8y3qrdw69xj24z5v** (hereinafter **bc1qth95**). The FBI used these records, along with open-source analysis of the Bitcoin blockchain, and the Ethereum blockchain, to trace Victim A and Victim B's funds. In summary, the tracing shows approximately \$784,940 of Victim A and Victim B's funds were transferred via intermediary addresses to the SUBJECT ASSETS and remained in the SUBJECT ASSETS at the time the addresses were frozen, on or about March 23, 2023.¹⁹

24. Crypto.com account records show between November 30, 2022 and March 17, 2023, \$2,375,237.36 was transferred from Victim A's bank account located at a United States-based financial institution headquartered in Cherry Hill, New Jersey to the Crypto.com correspondent account and credited to a Crypto.com customer account registered in Victim A's name or a Crypto.com customer account registered in Victim B's name.²⁰ Blockchain analysis²¹

¹⁹ The remaining funds were transferred through numerous digital currency addresses and co-mingled with funds from other known and unknown sources. For example, on February 6, 2023, 10 bitcoin and 156.933 ETH was transferred from Victim A's Athena Bitcoin account to Victim A's Exodus Wallet, converted to USDT (valued at approximately \$475,784), then transferred to 0xAb5c360FB1B2802a51307452fd004429C6d3Eac9 (0xAb5c360F), an address controlled by an unknown person. Those funds were co-mingled in 0xAb5c360F with funds (approximately \$4,303,447) transferred from 21 different addresses. Thereafter, the balance of 0xAb5c360F was depleted through a series of transfers (some round dollar, for example, \$400,000) to addresses controlled by unknown person(s). These transfers are contrary to the representations the scammers made to Victim A (that his funds were being held in a "treasury account") and make traditional tracing techniques largely ineffective in locating the misappropriated funds and in the identification of the individual(s) in control of those funds. Based on my training and experience, and the facts and circumstances of this investigation, this type of conduct is consistent with money laundering.

²⁰ Records obtained in this investigation indicate Victim A transferred approximately \$2,375,237 to Crypto.com and approximately \$1,660,000 to Athena Bitcoin, which is consistent with Victim A's statement he transferred between \$3 million and \$4 million at the direction of the scammers.

²¹ Unless otherwise noted, all dates and times referenced in the blockchain analysis are in UTC. All virtual asset amounts and USD conversion rate amounts are approximations.

shows the money belonging to Victim A and Victim B was transferred out of the Crypto.com accounts as follows:

- a. As detailed below, approximately 34,990 USDT from Victim A's Crypto.com account was transferred to Victim A's Exodus wallet and then to address **0x1bdd69 SUBJECT ASSET #1**.
 - i. On March 9, 2023, Victim A wired \$535,000 to his Crypto.com account.
 - ii. On March 13, 2023, approximately \$35,978 was converted to USDT.
 - iii. On March 13, 2023, approximately 34,990 USDT²² was transferred from Victim A's Crypto.com account to his Exodus wallet, **0x3fa26E**.
 - iv. On March 14, 2023, 34,990 USDT was transferred from **0x3fa26E** to private address **0x1bdd69 SUBJECT ASSET #1**.
 - v. According to blockchain analysis, the balance of **0x1bdd69 SUBJECT ASSET #1** prior to this transaction was 0 USDT.
- b. As detailed below, approximately 149,990 USDT was transferred from Victim B's Crypto.com account through a series of intermediary addresses to address **0x7c214b SUBJECT ASSET #2**.
 - i. On March 17, 2023, Victim A wired \$530,000 to Victim B's Crypto.com account.
 - ii. On March 17, 2023, approximately \$154,147 was converted to USDT.

²² Records from Crypto.com indicate 35,000 USDT was transmitted but Victim A's Exodus Wallet transaction history and blockchain analysis indicate only 34,990 was transferred.

- iii. On March 17, 2023, approximately 149,990 USDT²³ was transferred from Victim B's Crypto.com account to private address 0x3baDab55546A6D117f4A72901D9c346bBb6b8F8C (hereinafter **0x3baDab**). This address is suspected to be the Exodus wallet address of Victim B.²⁴
- iv. On March 17, 2023, approximately 149,990 USDT was transferred from **0x3baDab** to private address 0xD4A25F28D58130D78F548e89C4436f3b562cA34F (hereinafter **0xD4A25F INTERMEDIARY ADDRESS #1**).²⁵
- v. According to blockchain analysis, the balance of **0xD4A25F INTERMEDIARY ADDRESS #1** prior to this transaction was 0 USDT.
- vi. On March 17, 2023, approximately 149,990 USDT was transferred from **0xD4A25F INTERMEDIARY ADDRESS #1** to **0x7c214b SUBJECT ASSET #2**.
- vii. According to blockchain analysis, the balance of **0x7c214b SUBJECT ASSET #2** prior to this transaction was 0 USDT.

²³ Records from Crypto.com indicate 150,000 USDT was transmitted but blockchain analysis indicate only 149,990 was transferred.

²⁴ Victim A indicated he made transfers on behalf of his wife, Victim B, and that some of the same software (Exodus wallet) was installed on Victim B's phone. Victim A indicated Victim B's device had been cleaned and the wallet software was no longer available. Blockchain analysis indicates activity in the wallet began on December 8, 2022, which is around the time Victim A began engaging with the scammers. As such, your Affiant's belief is this address represents the private address in the Exodus wallet of Victim B.

²⁵ As described herein, **0xD4A25F** was utilized to transfer three discrete tranches of victim money. In each case, the balance of the address was 0 prior to the deposit of victim money, then fully liquidated.

- c. As detailed below, approximately 149,990 USDT was transferred from Victim A's Crypto.com account through a series of intermediary addresses to **0xcf95f2**

SUBJECT ASSET #3.

- i. On March 9, 2023, the same day Victim A wired \$535,000 to his Crypto.com account, approximately \$153,917 was converted to USDT.
 - ii. On March 9, 2023, approximately 149,990 USDT was transferred from Victim A's Crypto.com account to his Exodus wallet, **0x3fa26E**.
 - iii. On March 9, 2023, approximately 149,990 USDT was transferred from **0x3fa26E** to **0xD4A25F INTERMEDIARY ADDRESS #1**.
 - iv. According to blockchain analysis, the balance of **0xD4A25F INTERMEDIARY ADDRESS #1** prior to this transaction was 0 USDT.
 - v. On March 9, 2023, approximately 149,990 USDT was transferred from **0xD4A25F INTERMEDIARY ADDRESS #1** to **0xcf95f2 SUBJECT ASSET #3**.
 - vi. According to blockchain analysis, the balance of **0xcf95f2 SUBJECT ASSET #3** prior to this transaction was 0 USDT.
- d. As detailed below, approximately 149,990 USDT was transferred from Victim B's Crypto.com account to Victim B's suspected Exodus wallet to address **0xcf95f2**
- SUBJECT ASSET #3.**
- i. On March 18, 2023, the day after Victim A wired \$530,000 to Victim B's Crypto.com account, approximately \$154,350 was converted to USDT.

- ii. On March 18, 2023, approximately 149,990 USDT²⁶ was transferred from Victim B's Crypto.com account to Victim B's suspected Exodus wallet address, **0x3baDab**.
- iii. On March 18, 2023, approximately 149,990 USDT was transferred from **0x3baDab** to **0xcf95f2 SUBJECT ASSET #3**.
- iv. According to blockchain analysis, the balance of **0xcf95f2 SUBJECT ASSET #3** prior to this transaction was 149,990 USDT, which are funds traceable to Victim A as described above.
- e. As detailed below, approximately 149,990 USDT was transferred from Victim B's Crypto.com account to Victim B's suspected Exodus wallet to address **0xB8C348 SUBJECT ASSET #4**.
 - i. On March 20, 2023, three days after Victim A wired \$530,000 to Victim B's Crypto.com account, approximately \$154,188 was converted to USDT.
 - ii. On March 20, 2023, approximately 149,990 USDT²⁷ was transferred from Victim B's Crypto.com account to Victim B's suspected Exodus wallet address, **0x3baDab**.
 - iii. On March 20, 2023, approximately 149,990 USDT was transferred from **0x3baDab** to **0xB8C348 SUBJECT ASSET #4**.

²⁶ Records from Crypto.com indicate 150,000 USDT was transmitted but blockchain analysis indicate only 149,990 was transferred.

²⁷ Records from Crypto.com indicate 150,000 USDT was transmitted but blockchain analysis indicate only 149,990 was transferred.

- iv. According to blockchain analysis, the balance of **0xB8C348 SUBJECT ASSET #4** prior to this transaction was 29,990 USDT. This 29,990 USDT can be traced to the Crypto.com account of Victim C²⁸.
- f. As detailed below, approximately 149,990 USDT was transferred from Victim A's Crypto.com account through a series of intermediary addresses to address **0x9404a2 SUBJECT ASSET #5**.
 - i. On March 11, 2023, two days after Victim A wired \$535,000 to his Crypto.com account, approximately \$154,862 was converted to USDT.
 - ii. On March 11, 2023, approximately 149,990²⁹ USDT was transferred from Victim A's Crypto.com account to his Exodus wallet, **0x3fa26E**.
 - iii. On March 11, 2023, approximately 149,990 USDT was transferred from **0x3fa26E** to **0xD4A25F INTERMEDIARY ADDRESS #1**.
 - iv. According to blockchain analysis, the balance of **0xD4A25F INTERMEDIARY ADDRESS #1** prior to this transaction was 0 USDT.
 - v. On March 12, 2023 approximately 299,980 USDT was transferred from **0xD4A25F INTERMEDIARY ADDRESS #1** to **0x9404a2 SUBJECT ASSET #5**.

²⁸ Victim C is an elderly resident of Richmond, Virginia and was interviewed by the FBI on multiple occasions. Initially Victim C denied being a victim of a scam. Subsequently Victim C realized he had been defrauded. In subsequent interviews, Victim C acknowledged he had been defrauded and described a scheme similar to the one described in this affidavit. Victim C's total loss is unknown at this time, but believed to be several million dollars based on statements made to the FBI by Victim C and his associates and based on preliminary analysis of financial records obtained in the investigation.

²⁹ Records from Crypto.com indicate 150,000 USDT was transmitted but blockchain analysis indicate only 149,990 was transferred.

- vi. According to blockchain analysis, the balance of **0x9404a2 SUBJECT ASSET #5** prior to this transaction was 0 USDT. The amount of this transfer consists of 149,990 USDT belonging to Victim A, as described above, and 149,990 USDT traced to the Crypto.com address of Victim C.

25. Below is a table summarizing the tracing of Victim A and Victim B funds into the SUBJECT ASSETS at the time the accounts were frozen, on or about March 23, 2023:

Address	USDT	USD Equivalent (Approximate)
0x1bdd69	34,990	\$34,990
0x7c214b	149,990	\$149,990
0xcf95f2	299,980	\$299,980
0x9404a2	149,990	\$149,990
0xB8C348	149,990	\$149,990

26. Legal process was issued to Tether requesting information about the user(s) of **0x1bdd69, 0x7c214b, 0xcf95f2, 0xB8C348, and 0x9404a2** (the SUBJECT ASSETS). Tether responded to the legal process indicating it did not have any information about the person(s) utilizing the addresses.³⁰ At the request of law enforcement, on or around March 23, 2023, Tether temporarily restrained the assets in **0x1bdd69, 0x7c214b, 0xcf95f2, 0xB8C348, and 0x9404a2** (the SUBJECT ASSETS). Your Affiant's understanding is this process blocks the transfer of funds out of the addresses but allows for deposits into the addresses.

27. According to blockchain analysis, **0x1bdd69 SUBJECT ASSET #1** has been active since December 20, 2022. Between December 20, 2022 and March 2, 2023, **0x1bdd69** received three deposits totaling 246,973 USDT and sent four withdrawals totaling 246,973 USDT.

³⁰ According to the Tether response, the addresses are not owned or controlled by Tether and open source software can be used by any person to generate and uses addresses for transfers without involvement by Tether.

As of March 23, 2023, the balance in **0x1bdd69** was 34,990 USDT. No further transactions have occurred and as of the date of this affidavit, the balance remains 34,990 USDT.

28. According to blockchain analysis, **0x7c214b SUBJECT ASSET #2** has been active since February 28, 2023. Between February 28, 2023 and March 2, 2023, **0x7c214b** received one deposit in the amount of 367,200 USDT and sent one withdrawal in the amount of 367,200 USDT. On March 17, 2023, **0x7c214b SUBJECT ASSET #2** received a deposit in the amount of 149,990 USDT, traced to Victim B's suspected Exodus wallet address, as detailed above. As of March 23, 2023, the balance in **0x7c214b** was 149,990 USDT. No further transactions have occurred and as of the date of this affidavit, the balance remains 149,990 USDT.

29. According to blockchain analysis, **0xcf95f2 SUBJECT ASSET #3** has been active since October 31, 2022. Between October 31, 2022 and March 2, 2023, **0xcf95f2 SUBJECT ASSET #3** received seven deposits totaling 572,719 USDT and sent six withdrawals totaling 572,719 USDT. On March 9, 2023, **0xcf95f2 SUBJECT ASSET #3** received a deposit in the amount of 149,990 USDT traced to Victim A, detailed above. On March 18, 2023, **0xcf95f2 SUBJECT ASSET #3** received a deposit in the amount of 149,990 USDT from Victim B, detailed above. As of March 23, 2023, the balance in **0xcf95f2 SUBJECT ASSET #3** was 299,980 USDT. Since then, **0xcf95f2 SUBJECT ASSET #3** received three deposits totaling 320,104 USDT³¹. As of the date of this affidavit, the balance is 620,084 USDT.

³¹ 149,990 USDT was deposited on March 25, 2023 from private wallet address 0xb9C31e997DB9D7CB94A9FCB4d27526c3B4A44767. Through legal process, the FBI traced these funds to the Crypto.com account of Victim D. Victim D is an elderly resident of Ocala, Florida and was interviewed by your Affiant. According to Victim D, she was defrauded in a scheme similar to the one described in this affidavit. Victim D's total loss, based on statements to the FBI and blockchain analysis, is estimated to be approximately \$930,000. 170,014 USDT was deposited on March 28, 2023 from private wallet address 0xA333Ff74631b348733B8ef8047D684E6210bF0ee. 100 USDT was deposited on May 3, 2023

30. According to blockchain analysis, **0xB8C348 SUBJECT ASSET #4** has been active since December 20, 2022. Between December 20, 2022 and March 2, 2023, **0xB8C348 SUBJECT ASSET #4** received three deposits totaling 268,557 USDT and sent three withdrawals totaling 268,557 USDT. On March 14, 2023, **0xB8C348 SUBJECT ASSET #4** received a deposit in the amount of 29,990 USDT traced to the Crypto.com account of Victim C as detailed above. On March 20, 2023, **0xB8C348 SUBJECT ASSET #4** received a deposit in the amount of 149,990 USDT from Victim B as detailed above. As of March 23, 2023, the balance in **0xB8C348 SUBJECT ASSET #4** was 179,980 USDT. No further transactions have occurred and as of the date of this affidavit, the balance remains 179,980 USDT.

31. According to blockchain analysis, **0x9404a2 SUBJECT ASSET #5** has been active since November 26, 2022. Between November 26, 2022 and March 2, 2023, **0x9404a2 SUBJECT ASSET #5** received six deposits totaling 751,026 USDT and sent three withdrawals totaling 751,026 USDT. On March 12, 2023, **0x9404a2 SUBJECT ASSET #5** received a deposit in the amount of 299,980 USDT from **0xD4A25F INTERMEDIARY ADDRESS #1**. These funds were traced to Victim A and Victim C, as detailed below. As of March 23, 2023, the balance in **0x9404a2 SUBJECT ASSET #5** was 299,980 USDT. On March 28, 2023, **0x9404a2 SUBJECT ASSET #5** received a deposit in the amount of 149,990 USDT³² As of the date of this affidavit, the balance is 449,970 USDT.

from private wallet address 0x563a305E9a57e8e8aC33BAf4fF92dAF67F603dE5. As of the date of this affidavit, the individual(s) who sent these funds have not been identified.

³² 149,990 USDT was deposited on March 28, 2023 from private address 0x97F51d5EB6B6244ee31c5ffB0a13F3cbe390B8FC. Through legal process, the FBI traced these funds to the Crypto.com account of Victim E. Victim E is an elderly resident of La Quinta, California and was interviewed by your Affiant. According to Victim E, he was defrauded in a scheme similar to the one described in this affidavit. Victim E's total loss, based on statements to the FBI and blockchain analysis, is estimated to be approximately \$645,000.

32. According to blockchain analysis, **0xD4A25F INTERMEDIARY ADDRESS #1** has been active since February 24, 2023. Between February 24, 2023 and March 17, 2023, **0xD4A25F INTERMEDIARY ADDRESS #1** received fifteen (15) deposits totaling 2,441,949 USDT and sent thirteen (13) withdrawals totaling 2,441,949 USDT. As of March 23, 2023, the balance in **0xD4A25F INTERMEDIARY ADDRESS #1** was 0 USDT. On March 11, 2023, **INTERMEDIARY ADDRESS #1** received a deposit of 149,990 USDT from the Exodus wallet of Victim A (**0x3fa26E**). According to blockchain analysis, the balance of **0xD4A25F INTERMEDIARY ADDRESS #1** prior to this transaction was 0 USDT.

33. According to blockchain analysis, also on March 11, 2023, **0xD4A25F INTERMEDIARY ADDRESS #1** received a deposit of 149,990 USDT from Victim C. According to blockchain analysis, after this transfer the balance in **0xD4A25F INTERMEDIARY ADDRESS #1** was 299,980 USDT. On March 12, 2023, 299,980 USDT was transferred from **0xD4A25F INTERMEDIARY ADDRESS #1** to **0x9404a SUBJECT ASSET #5**.

34. This affidavit seeks seizure of the equivalent value of USDT as currently associated with **0x1bdd69**, **0x7c214b**, **0xcf95f2**, **0xB8C348**, and **0x9404a2**. Based on the specific tracing of USDT obtained fraudulently from Victim A, Victim B, Victim C, Victim D, and Victim E to these addresses, it is reasonable to believe at least some of the funds in these addresses are proceeds of criminal activity.

35. Based on my training and experience, I know individuals engaged in fraud sometimes move proceeds of criminal activity through multiple financial accounts, sometimes at a rapid pace, and often with no discernable legitimate purpose with the goal of concealing the true nature and source of the underlying funds. The blockchain analysis in this case demonstrates this; it shows the movement of the victim money, broken up and distributed through a series of

cryptocurrency addresses, to include the addresses **0x1bdd69 (SUBJECT ASSET #1)**, **0x7c214b (SUBJECT ASSET #2)**, **0xcf95f2 (SUBJECT ASSET #3)**, **0xB8C348 (SUBJECT ASSET #4)**, and **0x9404a2 (SUBJECT ASSET #5)** without any apparent legitimate economic purpose, which implies the purpose of the transactions was to conceal the nature, source, location, ownership and control of the proceeds. *See, e.g., United States v. Rodriguez*, 53 F.3d 1439, 1447-48 (7th Cir. 1995) (convoluted real estate transactions, from which intent to conceal or disguise may be inferred, also imply knowledge of illegal source).

CONCLUSION

36. I respectfully submit that this affidavit presents probable cause to believe that the private wallet(s) with addresses **0x1bdd69**, **0x7c214b**, **0xcf95f2**, **0xB8C348**, and **0x9404a2** received proceeds of the above-described fraud scheme perpetrated against Victim A, Victim B, Victim C, Victim D, and Victim E and, further, were used to commit concealment money laundering transactions in violation of 18 U.S.C. §§ 1956 (a)(1)(B)(i), (a)(2)(A), (a)(2)(B)(i), and (h) and the **SUBJECT ASSETS** are property involved in the underlying fraud. On that basis, I seek authority to obtain seizure warrants for the **SUBJECT ASSETS**.

/s/ Jayna Kadel (MDW with permission)

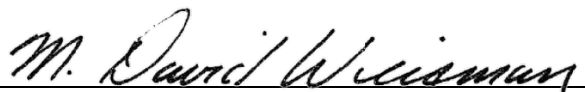
Applicant's Signature

JAYNA KADEL, Special Agent,

Federal Bureau of Investigation

Pursuant to Fed. R. Crim. P. 4.1, this Application is presented by reliable electronic means. The above-named agent provided a sworn statement attesting to the truth of the statements in the Application and Affidavit by telephone.

Date: 1/25/24



Judge's signature

M. David Weisman, U.S. 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 addresses referenced below. Tether shall effectuate this process by (1) burning the USDT tokens currently associated with the virtual currency addresses referenced below and (2) reissuing the equivalent value of USDT tokens to a U.S. law enforcement-controlled virtual currency account. Tether shall provide reasonable assistance in implementing the terms of this seizure warrant and take no unreasonable action to frustrate its implementation.

0x1bdd6956015976209e34e5f47C574A0f2cA9BD87 (SUBJECT ASSET #1),

0x7c214b43350B51B8C2B72c0C2b10b764Fc9774c6 (SUBJECT ASSET #2),

0xcf95f287E2856c34130B9D31859f3b2C29b45d50 (SUBJECT ASSET #3),

0xB8C348f248AD0493Ae2e6640D30ce3986413Af23 (SUBJECT ASSET #4), and

0x9404a2CBD5e46B91e814909c49fa071F31C86b7d (SUBJECT ASSET #5).

Exhibit 2

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

In the Matter of the Seizure of:

THE FUNDS ON DEPOSIT WITH TETHER at the following addresses:

0x1bdd6956015976209e34e5f47C574A0f2cA9BD87

(SUBJECT ASSET #1),

0x7c214b43350B51B8C2B72c0C2b10b764Fc9774c6

(SUBJECT ASSET #2),

0xcf95f287E2856c34130B9D31859f3b2C29b45d50

(SUBJECT ASSET #3),

0xB8C348f248AD0493Ae2e6640D30ce3986413Af23

(SUBJECT ASSET #4), and

0x9404a2CBD5e46B91e814909c49fa071F31C86b7d

(SUBJECT ASSET #5),

further Described in Attachment A.

**WARRANT TO SEIZE PROPERTY
SUBJECT TO FORFEITURE**

Case Number: 24 M 43

To: Federal Bureau of Investigation Special Agent JAYNA KADEL and any authorized law enforcement officer

An application by JAYNA KADEL, a Special Agent of the Federal Bureau of Investigation, requests that certain property be seized as being subject to forfeiture to the United States of America. The property is described as follows:

THE FUNDS ON DEPOSIT WITH TETHER at the following addresses:

0x1bdd6956015976209e34e5f47C574A0f2cA9BD87 (SUBJECT ASSET #1),

0x7c214b43350B51B8C2B72c0C2b10b764Fc9774c6 (SUBJECT ASSET #2),

0xcf95f287E2856c34130B9D31859f3b2C29b45d50 (SUBJECT ASSET #3),

0xB8C348f248AD0493Ae2e6640D30ce3986413Af23 (SUBJECT ASSET #4), and

0x9404a2CBD5e46B91e814909c49fa071F31C86b7d (SUBJECT ASSET #5),

further Described in Attachment A

I am satisfied that the affidavit and any recorded testimony establish probable cause to believe that the property so described is subject to seizure and that grounds exist for the issuance of this seizure warrant.

YOU ARE HEREBY COMMANDED to execute this warrant and seize the property specified on or before

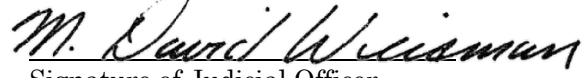
_____ (*not to exceed 14 days*), serving this warrant and making the seizure (in the daytime — 6:00

A.M. to 10:00 P.M.), leaving a copy of this warrant and receipt for the property seized, and prepare a written inventory of the property seized and promptly return this warrant to the undersigned United States Magistrate Judge as required by law.

January 25 2024 at 4:28 p.m.
Date and Time of Issuance

M. David Weisman, U.S. Magistrate Judge
Name & Title of Judicial Officer

at Chicago, Illinois
City and State


Signature of Judicial Officer

RETURN

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of:

Inventory of the property seized:

CERTIFICATION

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing Agent/Officer signature

Printed name and title

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 addresses referenced below. Tether shall effectuate this process by (1) burning the USDT tokens currently associated with the virtual currency addresses referenced below and (2) reissuing the equivalent value of USDT tokens to a U.S. law enforcement-controlled virtual currency account. Tether shall provide reasonable assistance in implementing the terms of this seizure warrant and take no unreasonable action to frustrate its implementation.

0x1bdd6956015976209e34e5f47C574A0f2cA9BD87 (SUBJECT ASSET #1),

0x7c214b43350B51B8C2B72c0C2b10b764Fc9774c6 (SUBJECT ASSET #2),

0xcf95f287E2856c34130B9D31859f3b2C29b45d50 (SUBJECT ASSET #3),

0xB8C348f248AD0493Ae2e6640D30ce3986413Af23 (SUBJECT ASSET #4), and

0x9404a2CBD5e46B91e814909c49fa071F31C86b7d (SUBJECT ASSET #5).