UNITED STATES DISTRICT COURT
DISTRICT OF MAINE

UNITED STATES OF AMERICA, Plaintiff, 470,773 USDT ASSOCIATED WITH VIRTUAL CURRENCY ADDRESS 0x55Df4Ecd9066C417103F59d3eCc9B309Dedfd131 AND SEIZED ON MARCH 6, 2024, Defendant *in Rem*.	No: 1-24-cv-

VERIFIED COMPLAINT FOR FORFEITURE *IN REM*

Plaintiff, the United States of America, brings this complaint and alleges as follows in accordance with Supplemental Rule G(2) of the Federal Rules of Civil Procedure:

NATURE OF THE ACTION

1. This is a civil forfeiture action *in rem*, as authorized by 18 U.S.C. §§ 981 and 983, in which the United States of America alleges that 470,773 USDT[1] associated with the virtual currency address 0x55Df4Ecd9066C417103F59d3eCc9B309Dedfd131 and seized by the Federal Bureau of Investigation on March 6, 2024 (the "Defendant Property" or the "defendant in rem") is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C) because it is property, real or personal, which constitutes or is derived from proceeds traceable to wire fraud or wire fraud conspiracy, in violation of 18 U.S.C. §§ 1343 and 1349. Further, the Defendant Property is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A) because it is property, real or personal, involved in money laundering transactions in violation of 18 U.S.C. §§ 1956 and 1957, or

1 "USDT" tokens, often referred to as "Tether," are a form of cryptocurrency issued by Tether Limited.

is property traceable to such property.

DEFENDANT IN REM

2. The defendant in rem consists of 470,773 USDT associated with the virtual currency address 0x55Df4Ecd9066C417103F59d3eCc9B309Dedfd131 and seized by the Federal Bureau of Investigation on March 6, 2024.[2]

3. On January 19, 2024, the United States sought and was granted a seizure warrant for the defendant in rem. On March 6, 2024, Tether transferred the defendant in rem to the custody of the Federal Bureau of Investigation.

4. The defendant in rem is presently in the custody of the United States Marshals Service. The defendant in rem is held in one or more virtual currency wallets under the control of the United States Marshals Service.

JURISDICTION AND VENUE

5. This Court has jurisdiction over this action pursuant to 28 U.S.C. §§ 1345 and 1355.

6. Venue is proper in this district pursuant to 28 U.S.C. § 1355(b)(1)(A) because acts or omissions giving rise to the forfeiture occurred in the District of Maine. Further, venue is proper in this district pursuant to 28 U.S.C. § 1395(a), which permits a civil proceeding for forfeiture to "be prosecuted in the district where it accrues or the defendant is found."

---

2 The manner in which 470,773 USDT associated with that virtual currency address was seized—by way of Tether providing an equivalent amount of USDT tokens to 470,773 USDT associated with the virtual currency address at the time of seizure—is explained further below.

DEFINITIONS AND BACKGROUND

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

8. 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[3] to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are Bitcoin, Litecoin, Ether, and USDT tokens. 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,

3 Fiat currency is currency issued and regulated by a government such as the U.S. Dollar, Euro, or Japanese Yen.

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.

a. Although cryptocurrencies such as Bitcoin and Tether's USDT have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering and is an oft-used means of payment for illegal goods and services.

9. 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. Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives.

10. Tether Limited is a company registered to do business in the British Virgin Islands that manages the smart contracts and the treasury (*i.e.*, the funds held in reserve) for USDT tokens, which are a form of cryptocurrency. USDT tokens are stablecoins pegged to the value of the United States dollar. Tether Limited purports to maintain $1.00 of U.S. Currency in reserve for each USDT issued. Essentially, Tether is

the sole entity involved in the issuance of USDT tokens.

a. As of March 6, 2024, the date of the seizure discussed herein, one USDT was worth approximately $1.00. One USDT continues to be worth approximately $1.00 as of the date of this Verified Complaint.

b. USDT tokens are issued on various blockchains. In this case, the tokens involved are ERC-20 USDT, which operate on the Ethereum blockchain.

11. A blockchain is a digital ledger run by a decentralized network of computers referred to as "nodes." Each node runs software that maintains an immutable and historical record of every transaction utilizing that blockchain's technology. Many digital assets, including virtual currencies, publicly record all of their transactions on a blockchain, including all of the known balances for each virtual currency address on the blockchain.[4] Blockchains consist of blocks of cryptographically signed transactions, and blocks are added to the previous block after validation and after undergoing a consensus decision to expose and resist tampering or manipulation of the data. There are many different blockchains used by many different virtual currencies. For example, Bitcoin in its native state exists on the Bitcoin blockchain, while Ether (or "ETH") exists in its native state on the Ethereum network. USDT tokens are issued on various blockchains including, for example, the Ethereum network.

12. A transaction hash, also called a transaction ID, is a unique string of characters which identifies a specific transaction on the blockchain—akin to a serial

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

number or accounting journal entry number. A transaction hash is assigned to a transaction when it is added to the blockchain, and it is generated by applying a hash function to the transaction details, including the sender's address, the receiver's address, and the amount of virtual currency being sent. Transaction hashes can be found on blockchain explorers and can be used to verify and track transactions.

13. Cryptocurrency mining is the process that several virtual currencies, including Bitcoin, use to verify and add blockchain transactions to a public ledger (*e.g.*, the Bitcoin blockchain). Miners operate specialized computers that compete to perform mathematical problems needed to validate blockchain transactions. The first miner to accurately solve the problem authorizes a block of transactions, and as a reward, receives newly released or "mined" virtual currency that is native to the specific network or blockchain.

14. A transaction fee is a fee paid by the party sending virtual currency on a blockchain to reward miners and/or validators for verifying and validating transactions. Transaction fees vary by blockchain and can fluctuate based on factors such as blockchain network traffic and transaction sizes. Senders of virtual currency can increase the transaction fees that they pay to have their transactions confirmed faster by miners and/or validators. Transaction fees are generally paid in a blockchain's native token (*e.g.*, bitcoin on the Bitcoin blockchain). On the Ethereum network, these transaction fees are called "gas fees." Gas fees are transaction costs paid in Ether ("ETH"), or its fraction, gwei. These fees serve as a form of remuneration for validators who maintain and secure the network. Gas fees fluctuate based on supply, demand, and network capacity, and may increase during periods of network congestion.

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

16. A virtual currency address is an alphanumeric string that designates the virtual location on a blockchain where virtual currency can be sent and received. A virtual currency address is associated with a virtual currency wallet.

17. A virtual currency wallet (*e.g.*, a hardware wallet, software wallet, or paper wallet) stores a user's public and private keys, allowing a user to send and receive virtual currency stored on the blockchain. Multiple virtual currency addresses can be controlled by one wallet. 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 key or address. 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 represented as a case-sensitive string of letters and numbers of varying character lengths. 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. Generally, only the holder of an address's private key can authorize any transfers of cryptocurrency

from that address to another cryptocurrency address.

i. A hardware wallet is a physical, removable device that stores a user's private keys and can be connected to a computer when a user wishes to use the keys stored on the wallet for virtual currency transactions. Hardware wallets can be secured with PINs and passphrases and can be backed up or regenerated with a recovery phrase. Trezor and Ledger are some examples of the types of hardware wallets on the market.

ii. A hosted wallet, also known as a custodial wallet, is a virtual currency wallet through which a third party, *e.g.*, a virtual currency exchange, holds a user's private keys. The third party maintains the hosted wallet on its platform akin to how a bank maintains a bank account for a customer, allowing the customer to authorize virtual currency transactions involving the hosted wallet only by logging into/engaging with the third party's platform.

iii. A multi-signature wallet (or "multisig" wallet) (also sometimes called "multisig vaults" or "safes") requires two or more private key signatures to authorize transactions. Multi-signature wallets requiring more than two private key signatures can be designed so a majority of keys is needed to authorize transactions.

iv. A paper wallet is an offline paper record of a virtual currency wallet's public and private keys. Paper wallets can include barcodes (*e.g.*, a QR code) along with their alphanumeric strings. It is literally private keys printed on a piece of paper.

v. A software wallet is an internet-connected virtual currency wallet in the form of a software application on a desktop or mobile device or a web-based platform accessible through a web browser. The software will store and usually encrypt the user's public and private keys.

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

vii. 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).

18. A private key is a cryptographic key that is uniquely associated with an entity and not made public. In the blockchain and virtual currency context, virtual currency addresses are controlled using a unique corresponding private key, the equivalent of a password, which is needed to access the funds associated with the address. Generally, only the holder of an address's private key can authorize a transfer of virtual currency from that address to another address.

19. A public key is a cryptographic key that is uniquely associated with a person or entity and is designed to be made public. The public key is paired with, and derived from, a private (secret) key. However, knowing the public key does not reveal

any information about the private key. In the blockchain and virtual currency context, a virtual currency address is the hashed value of a public key and acts as an identifier on a blockchain.

20. A key pair, in cryptography, refers to a private key and its corresponding public key. A key pair is used with a public-key algorithm.

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

a. The information contained herein is based, in part, on blockchain analysis using the commercial blockchain analysis tool Chainalysis. Commercial blockchain analysis tools supplement open source blockchain data by applying heuristics or manual investigations to enhance the process of blockchain analysis. A cluster (or grouping of addresses) in these tools is a collection of addresses where the tool vender assesses one entity controls them.

22. A blockchain explorer, also called a block explorer, is software that operates as a blockchain search engine for users to search and review transactional data for any addresses on a particular blockchain. A blockchain explorer uses an application programming interface and blockchain nodes to draw data from a blockchain and uses a database to arrange, visualize, and present the data to a user in a searchable format. This data can include average transaction fees, hash rates, and block size.

23. The term domain spoofing refers to a process by which cybercriminals seek to persuade victims that a web address or email address belongs to a legitimate and generally trusted company, when in fact it links the user to a fraudulent site controlled by a cybercriminal. The fraudulent site is referred to as a spoofed domain.

24. Cryptocurrency investment schemes (also known as "cryptocurrency confidence schemes" and previously referred to as "pig butchering" schemes) are schemes where criminal actors engage in social engineering, which allow the criminal actors to steal victims' funds through virtual currency payments and/or fraudulent investments. The phrase "pig butchering" is translated from the Chinese "shāzhūpán" and refers to a scam in which the victim is "fattened up prior to slaughter." These scams typically involve four stages. First, a perpetrator will use a fictious identity and cold-contact a victim, often via text message or messaging application, social media, a dating application, or other communication platform. Oftentimes, the perpetrator will pretend to have contacted the wrong number but will continue communicating with the victim. Second, the perpetrator will establish a relationship and build trust with the victim by continuing to message over days, weeks, or months. Third, the scammer will concoct a narrative to induce the victim to send a

series of payments in the form of virtual currency. Common narratives include lucrative investment opportunities or emergencies necessitating funds. Many perpetrators will convince victims to use fraudulent websites or applications, controlled by scammers, to invest in virtual currency. Perpetrators coach victims through the investment process, show them fake profits, and encourage victims to invest more. In the fourth stage, perpetrators disengage victims once they have stolen their funds. In scenarios when victims stop sending more payments, the perpetrator cuts off all contact. In schemes involving fraudulent investment platforms, victims are told they need to pay a fee or tax when they attempt to withdraw their money. Victims are then unable to get their money back from perpetrators, even if they pay the fake fees or taxes.

FACTUAL BASIS FOR FORFEITURE

I. The Scheme to Defraud

25. On about October 20, 2022, the FBI Resident Agency office in Portland, Maine became aware of Victim 1, who then resided in Maine. Victim 1 provided information indicating that they were the victim of conduct consistent with a cryptocurrency investment scheme.

26. Victim 1 reported that they met a person—whom they understood to be a female—on Tinder, an online dating site. Though she reportedly used the screen name

"Jessica," Victim 1 understood the person's "real name" to be Chie Aoi ("Aoi").[5, 6, 7]

27. Aoi used the email address wenyongcheng1985[@]gmail.com.[8] Google records indicate that the subscriber associated with this email address was an individual named "Chief Aoi" and that the email account was accessed during the relevant period from IP addresses resolving to China Mobile Limited, a communications service provider based in Hong Kong. Aoi used the email address wenyongcheng1985[@]gmail.com to contact Victim 1 as late as January 5, 2023, when Aoi emailed to inquire how Victim 1 was doing.

28. After meeting on Tinder, Victim 1 reported communicating with Aoi exclusively over Telegram, a messaging application. Aoi gained Victim 1's trust and

---

5 Because the person or persons acting as "Chie Aoi" or "Jessica" has not been definitively identified, they are referred to herein as "Aoi" and using she/her/hers pronouns. Personas like Aoi can be, and often are, played by more than one perpetrator engaged in the cryptocurrency confidence scheme.

6 In an October 2022 email to Victim 1, the user of the wenyongcheng1985[@]gmail.com address stated, "Hello, yes, I'm Qian Hui[.]"

7 Victim 1 initially reported to the Federal Bureau of Investigation that the person who victimized them and led them into the fraud scheme was an individual in Maine who worked for the same company from which Victim 1 had retired. Victim 1 indicated that Victim 1 had spoken with that individual by phone sometime in June 2022, at which time that individual proposed cryptocurrency trading for Victim 1 to make more money. Victim 1 indicated that the individual had Victim 1 create a Telegram account and the two subsequently communicated via Telegram, with the individual using the name "Jessica." Victim 1 indicated that the individual was the one responsible for directing Victim 1 to use "Trust" and, later, Crypto.com, and directing Victim 1's subsequent transfers in the fraud scheme. Victim 1's spouse was present for the interview during which Victim 1 reported this information to the Federal Bureau of Investigation. Subsequently, on about November 29, 2022, Victim 1 corrected their initial report, revealing they met the perpetrator over the dating application Tinder. Victim 1 cited embarrassment, and the desire to not reveal the true source of their victimization to their spouse, as the reason for their initial claim. Victim 1 disclosed that the person Victim 1 had initially identified as the perpetrator was never involved in the scam.

8 Brackets are placed within certain email addresses and URLs in this Verified Complaint to prevent inadvertent connections.

deceived Victim 1 into making what Victim 1 believed were cryptocurrency "investments," or paying fees to withdraw from the investments. Instead, Aoi induced Victim 1 to transfer cryptocurrency to addresses controlled by the perpetrators of the fraud.

29. In their communications, Aoi convinced Victim 1 to buy cryptocurrency, at first directing Victim 1 to start with small investments through a cryptocurrency custodian "Trust," before directing Victim 1 to use Crypto.com.[9]

30. Aoi eventually directed Victim 1 to use a purported online trading platform, identified as FXCMPRO[.]CC, to "invest" Victim 1's cryptocurrency. The uniform resource locator ("URL") for the FXCMPRO[.]CC platform changed often, but Aoi knew how to access each new site and directed Victim 1 to it. According to screen captures of some of Victim 1's interactions with the purported platform or with "Customer service," the purported platform was also located at, or used, the domains GXUHIEWBCP[.]BUZZ and MMYNSMAA[.]XYZ at different points. Aoi referred to the platform as the "fast trading site."

31. Based on Aoi's statements, Victim 1 understood the platform to be the FXCM Exchange. FXCM, or Forex Capital Markets, is a real retail foreign exchange broker. However, the FXCMPRO[.]CC sites to which Aoi directed Victim 1 were not truly associated with FXCM—rather, Aoi engaged in domain spoofing. Aoi convinced Victim 1 that the web addresses belonged to a legitimate company, when in fact the addresses to which Aoi sent Victim 1 linked Victim 1 to a fraudulent site controlled by Aoi and/or

9 "Trust" likely refers to Trust Wallet, a non-custodial wallet software.

other cybercriminals.

a. A search through a publicly available domain search tool demonstrates that the FXCMPRO[.]CC domain was created on July 2, 2022, through a domain registry service company based in Arizona, near in time to the use of that domain in the fraud scheme.

b. A search through a publicly available domain search tool demonstrates that the GXUHIEWBCP[.]BUZZ and MMYNSMAA[.]XYZ domains were created on August 10, 2022, and April 22, 2022, respectively, through the same Arizona based registry service, near in time to the use of those domains in the fraud scheme.

32. Aoi further directed Victim 1 to send Victim 1's "investments" (or fees related to withdrawing Victim 1's "investments") on FXCMPRO[.]CC, from Victim 1's Crypto.com account to three addresses purportedly associated with the fake FXCMPRO[.]CC exchange:

a. A virtual currency address ending in d131 ("VCA d131");

b. A virtual currency address ending in 0c48 ("VCA 0C48"); and

c. A virtual currency address ending in 91Fc ("VCA 91Fc").

33. "Customer service" for the purported platform directed Victim 1 to direct at least two transactions to VCA d131.

34. Victim 1 reported using a bank account under the name of a relative's estate—of which Victim 1 is or was the executor—to fund their initial "investment." Victim 1 then reportedly used money from their joint investment account as well as their personal bank accounts and their joint bank accounts with their spouse, Victim 2, to buy

cryptocurrency and fund subsequent "investments" or fees related to withdrawals.

35. Based upon bank records, as used herein, the bank account under the name of a relative's estate is referred to as "Bank Account 1." The joint investment account is referred to as "Investment Account 1." Victim 1's personal bank accounts are referred to as "Bank Account 2" and "Bank Account 5." Victim 1's joint bank accounts with Victim 2 are referred to as "Bank Account 3" and "Bank Account 4."

36. Victim 1 reportedly did not send funds to VCA 91Fc.

37. As reflected in records, Victim 1's wire transfers and ACH debits into their Crypto.com account from Bank Account 1, Bank Account 2, Bank Account 3, and Bank Account 5 are summarized below.[10] The transfers amount to $895,600 in total, with the majority of funds ultimately transferred to VCA d131 and VCA 0c48.

Date	**Transfer Source Account**	**Amount**
6/23/2022	Bank Account 1	$ 1,500.00
7/8/2022 [11]	*Bank Account 1*	$ 3,325.00
7/25/2022	Bank Account 1	$ 100.00
8/8/2022	Bank Account 2	$ 50,000.00
8/16/2022	Bank Account 5	$ 16,000.00
8/22/2022	Bank Account 2	$ 50,000.00
8/24/2022	Bank Account 3	$ 50,000.00
8/26/2022	Bank Account 5	$ 50,000.00
8/30/2022	Bank Account 3	$ 50,000.00

10 The Federal Bureau of Identification identified approximately $47,000 in payments made to MCB Foris/Crypto.com that were debit card purchases, which are not scheduled below. These debit card purchases also came from Bank Account 6, an account in Victim 1's name. The Crypto.com activity identified during the investigation showed approximately $896,000 in vIBAN (virtual Bank Account Number) purchases, matching the approximate total of ACH and wire transfers identified in bank records.

11 Records suggest this transaction was returned/reversed shortly after it took place, with an incoming transfer of $3,325.00 on July 13, 2022.

9/1/2022	Bank Account 3	$ 50,000.00
9/2/2022	Bank Account 3	$ 50,000.00
9/7/2022	Bank Account 3	$ 50,000.00
9/12/2022	Bank Account 2	$ 23,000.00
9/12/2022	Bank Account 3	$ 25,000.00
9/14/2022	Bank Account 3	$ 50,000.00
9/16/2022	Bank Account 2	$ 40,000.00
9/20/2022	Bank Account 3	$ 60,000.00
9/21/2022	Bank Account 3	$ 60,000.00
9/23/2022	Bank Account 3	$ 120,000.00
10/5/2022	Bank Account 3	$ 50,000.00
10/5/2022	Bank Account 3	$ 50,000.00

38. Records show that Victim 1's June 23, 2022 transfer from Bank Account 1 was by "ACH DEBIT" to "FORIS INC MCB PAYMENT." Records further show that Victim 1's transfers from Bank Account 2 and Bank Account 3 were generally to "Mcb Foris." Metropolitan Bank Holding Corporation is the holding company for Metropolitan Commercial Bank and trades on the New York Stock Exchange under the symbol MCB. Foris DAX, Inc. does business as Crypto.com. It appears MCB serviced Foris DAX, Inc. by receiving the wire transfers on behalf of Foris DAX, Inc.

39. Victim 1 reported observing their "investment" into FXCM purportedly grow very quickly from $100,000 to $300,000 and wished to make a withdrawal. Victim 1 was told to pay $54,000 in taxes in order to withdraw the money—Aoi told Victim 1 this was standard procedure and that Victim 1 should do it. Victim 1 then paid the money. Thereafter, Victim 1 was told they were required to make additional payments for different reasons, such as needing to "recharge," "top up" to "upgrade the membership business," or pay a platform management fee, an account activation fee, or a refundable risk deposit fee. For example, according to screen captures provided by

Victim 1 and/or Victim 2, Victim 1 had the following exchanges with "Customer service" at the purported platform using the address mmynsmaa[.]xyz:

a. On about September 21, 2022, Victim 1 told "Customer service":

> I can send the funds now to open the green channel. 48888USDT to Ox55Df4Ecd9066C417103F59d3eCc9B309Dedfd131?

Victim 1 followed up with:

> Please confirm[.]

"Customer service" responded:

> Hello: After the recharge is completed, please take a screenshot and check with the customer service[.]

"Customer service" later stated:

> Hello, the system is querying for you, please be patient!
>
> Hello: The system has detected that your valid deposit of 48888USDT has been sent to your account. If you need to open the green channel to withdraw funds, please pay the platform management fee of 8888USDT first, and then open the green channel to release the account funds after recharging 48888USDT.

"Customer service" later stated:

> Hello: the system has received 8888USDT platform management fee, please deposit 48888USDT to open the green channel to release funds.

b. On about September 22, 2022, Victim 1 stated:

> I have just sent you the platform management fee of 8888USDT and the green channel management fee of 48888USDT combined in a single payment of 57776USDT[.]

Victim 1 included what appears to be a screen capture regarding

"Withdraw USDT (ERC20)" in the amount of 57,786.00 USDT.

"Customer service" then stated:

> Hello, the system is querying for you, please be patient!
>
> Hello; the system has received your default effective recharge of 57776USDT and has sent it to your account for you. If you need to open a green channel, please apply to the online customer service for the corresponding fee to complete the fund withdrawal business[.]
>
> Hello: the system verified that it has not received your application for opening the green channel fee. Please apply to the customer service for the green channel fee and then recharge the funds.

Upon Victim 1's further inquiry, including whether this was a hoax or scam, "Customer service" responded:

> Hello: you just inquired about the fees, but did not apply for green channel business[.]
>
> You need to activate the business before the system will verify it for you[.]

"Customer service" further explained that the system had not received Victim 1's application, as Victim 1 had "only consulted the fees before . . . ."

c. On about September 25, 2022, Victim 1 was told by "Customer service":

> Hello, yes, please send to the following address [VCA d131][.]

Victim 1 responded with what appears to be a screen capture regarding "Withdraw USDT (ERC20)" in the amount of 26,339.00 USDT.

d. On a date not captured in the screen capture, Victim 1 was told by "Customer service":

> Hello, because your friend did not verify the funds, the return of funds failed, the system has defaulted to your valid recharge, and 29829USDT has been sent to your account. Please recharge 26329USDT and pay 26329USDT margin to release the account. (Due to multiple errors in your account. For the security of your account, please complete the recharge within 72 hours)

e. On about October 4, 2022, Victim 1 was told by "Customer service":

> Hello, the system detected that the identity came from a third party top-up [Chinese characters] (Chie Aoi), and since she did not receive the funds, the return of the funds failed.

f. On about October 4, 2022, Victim 1 was told by "Customer service":

> After the recharge is completed, please check the screenshot with the customer service. After the verification is successful, your funds will reach the designated account[.]

Victim 1 replied:

> And send to the same address as before: [VCA d131][.]

"Customer service" replied:

> Hello yes. After the recharge is complete, please check with the online customer service.

g. On about October 7, 2022, Victim 1 was told by "Customer service":

> Hello, the return of funds has been completed. Since your platinum membership business has expired, please renew your platinum membership by 58,000 USDT, and the platinum membership fee will be returned to your account within 24 hours. Your funds will be released after the upgrade is complete.

Victim 1 replied:

> How is this even possible? I have asked over aand [sic] over about additional fees, additional payments and you said there would be none.

h. On a date not captured in the screen capture, Victim 1 told "Customer service":

> I would like to send you now 52658 USDT top off to complete the fund withdrawal process. Are you ready?

On about October 7, 2022, "Customer service" responded:

> Hello, after the recharge is complete, please take a screenshot and check with the customer service.

Victim 1 then responded with what appears to be a screen capture regarding "Withdraw USDT (ERC20)" in the amount of 52,668.00 USDT.

40. Each time Victim 1 was told to make additional payments, Victim 1 reported that they would contact Aoi, who would reassure Victim 1 that it was standard procedure. Victim 1 continued to make the "required" payments. Despite making such payments, Victim 1 reported they were not able to withdraw their funds.

41. Victim 1 believed their "investments" into the cryptocurrency scheme went to two Tether addresses, which ended in "131" and "c48."

II. Initial Tracing of Funds and Request to Freeze VCA d131

42. Victim 2, Victim 1's spouse, reported to the Federal Bureau of Investigation that they discovered the scam when they came across a credit card charge for approximately $10,000 and asked Victim 1 about it. Victim 1 told Victim 2 of the scheme, though Victim 1 described the scammer as an employee of Victim 1's former employer.[12]

43. Victim 2 hired a cryptocurrency forensic firm ("Tracing Firm") to help the couple track and recover their funds. Tracing Firm's blockchain analysis traced a portion of their funds to VCA d131 and VCA 0c48 and showed that VCA d131 held the larger balance of Victim 1 and Victim 2's funds. Pursuant to a request by Tracing Firm, Tether agreed to temporarily freeze the contents of VCA d131 for a short period. According to

12 Victim 2 reported that Victim 1 had disclosed connecting with that individual in July 2022 and maintaining regular contact over the next several weeks, until Victim 1 had lost approximately $880,000 through the scam.

correspondence between Tether and Tracing Firm, at the time of the temporary freeze on October 19, 2022, the balance in VCA d131 was 861,259 USDT.

44. On October 21, 2022, the Federal Bureau of Investigation also transmitted a request to Tether for that entity to voluntarily freeze the contents of VCA d131. On October 24, 2022, the Federal Bureau of Investigation learned that Tether had frozen the contents of VCA d131 and that the address held a balance of 861,260 as of that day.

45. On about November 9, 2022, the Federal Bureau of Investigation received notification from Tether that it had received a claim on VCA d131 from an individual under the name "cheng辰" and using the email address c7529955820[@]gmail.com.

46. On about November 11, 2022, the Federal Bureau of Investigation also received an email written in Chinese from the email address c7529955820[@]gmail.com, with the associated name of "cheng辰." The Federal Bureau of Investigation determined the message stated, in part and as translated:

> Hello! My USDT-ERC20 malfunctioned on October 19, 2022. Only transfer-in is allowed at this transaction address, not transfer-out. Prompt error 10560 when transferring out: The transaction you want to send will fail to execute. To avoid losing miners' fees, please check the data to try again.
> The wallet address is 0x55Df4Ecd9066C417103F59d3eCc9B309Dedfd131. Being blacked out by your contract address makes it impossible to transfer money. Please solve my problem. I am a businessman; I do not know what happened! These are all the money I've worked so hard to earn!!!

47. According to records provided by Google, Inc., the email account for address c7529955820[@]gmail.com was created on about October 25, 2022. Records also showed that the email account was accessed on about October 25, 2022, from an Internet Protocol ("IP") address resolving to a regional IP administrator in the United

Kingdom, and that the account's recovery SMS number began with country code +44. That country code is assigned to the United Kingdom.

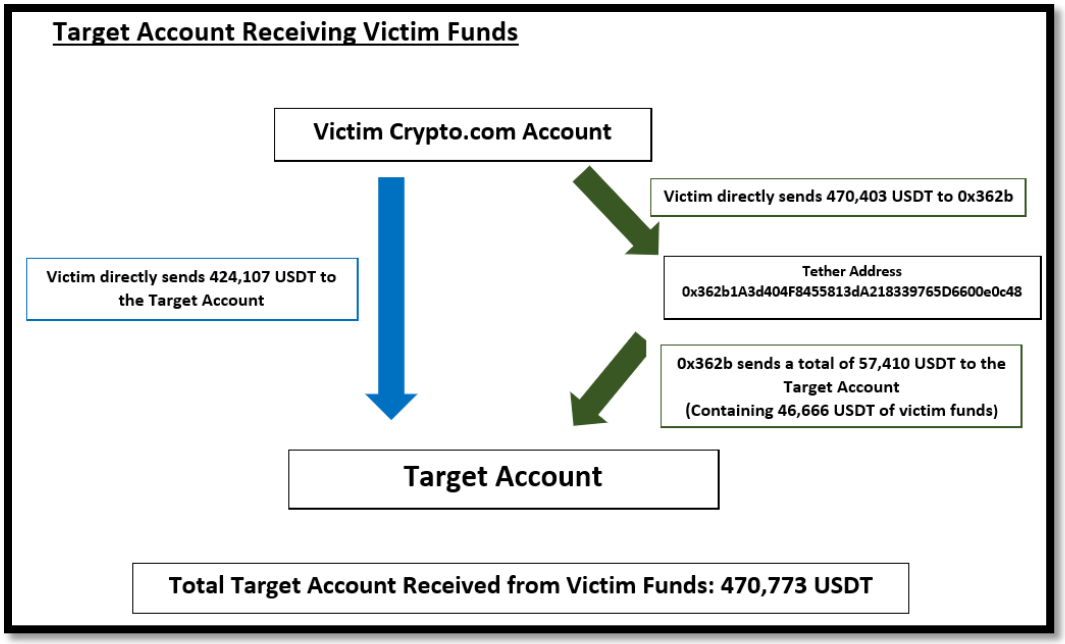
III. Tracing Victim 1 and Victim 2's Funds to VCA d131

48. Victim 1 was deceived into sending several ACH and wire transfers from the bank accounts described above to their account with the cryptocurrency exchange Crypto.com. From there, Victim 1 was further deceived into transferring USDT tokens on the Ethereum blockchain from Victim 1's Crypto.com account to VCA d131 and VCA 0c48.

49. The Federal Bureau of Investigation has access to one or more proprietary software tools that analyze financial transactions on the blockchain. Using this software, data from the Ethereum blockchain, manual tracing on the blockchain, and information provided by Victim 1, Victim 2, and Tracing Firm, a forensic accountant with the Federal Bureau of Investigation analyzed the flow of funds from Victim 1's Crypto.com account and traced multiple USDT transfers from that Crypto.com account to VCA d131 and VCA 0c48.

50. The Federal Bureau of Investigation traced approximately 470,773 USDT from Victim 1's Crypto.com account to VCA d131 through both direct and indirect deposits into VCA d131. These transfers are visually summarized as follows[13]:

13 The Target Account referenced in the visual summary is VCA d131. The "0x362b" address referenced in the visual summary is VCA 0c48.



a. The deposits from Victim 1's Crypto.com account directly into VCA d131 occurred from on about September 14, 2022, through on about October 6, 2022.

b. The deposits from Victim 1's Crypto.com account into VCA 0c48 occurred from on about July 7, 2022, through on about September 13, 2022. After receiving 470,403 USDT in Victim 1's funds and additional comingled funds from other sources, the controller of VCA 0c48 remitted a portion of Victim 1's funds and other comingled funds—a total of 57,410 USDT, including 46,666 USDT of Victim 1's funds, as referenced in the above chart—in two transfers to VCA d131 on about September 13, 2022.

c. The phrase "indirect deposit" refers to the transfer of funds from Victim 1's Crypto.com account to VCA 0c48 and the subsequent transfer of a portion of those funds to VCA d131.

d. Specifically, as shown above, 424,107 USDT is traceable from Victim 1's Crypto.com account as directly transferred into VCA d131 as part of the fraud scheme. A further 46,666 USDT is traceable from Victim 1's Crypto.com account as transferred into VCA d131 by way of transfer through VCA 0c48.

51. The following chart details transfers from the Crypto.com account to VCA d131 and VCA 0c48:[14]

Date	7/7/22 19:19
USDT Amount	1,454.81
Sent to wallet address	0x362b1a3d404f8455813da218339765d6600e0c48
Transaction Hash	0x666fdcba41385c14285950acc549ad5ef3053dce1591c055a3b080d1b78c0316

Date	7/29/22 17:43
USDT Amount	6,025.00
Sent to wallet address	0x362b1a3d404f8455813da218339765d6600e0c48
Transaction Hash	0x63aeb2ab61e3fc3cf568267cc6cd6d4e7abc1b8c33ed192ad2aed13285e67b43

Date	8/9/22 15:06
USDT Amount	48,683.03
Sent to wallet address	0x362b1a3d404f8455813da218339765d6600e0c48
Transaction Hash	0x56df83f680033cd898a9df225e77de2361f9dce242332b6582b26433f552f8b6

Date	8/12/22 23:16
USDT Amount	13,637.79
Sent to wallet address	0x362b1a3d404f8455813da218339765d6600e0c48
Transaction Hash	0x44a4a31ec52bc32819275b257e77ba9d4e129623cb821200b520770606208740

14 Unless otherwise noted, all cryptocurrency-related dates and times referenced are in UTC. All virtual currency amounts and US dollar conversion rate amounts are approximate.

Date	8/16/22 19:06
USDT Amount	15,595.87
Sent to wallet address	0x362b1a3d404f8455813da218339765d6600e0c48
Transaction Hash	0x00754e83397aaf704cf319fd9feba4b26b87261d972b30e0e49c0b14366b4e02

Date	8/23/22 3:50
USDT Amount	48,717.52
Sent to wallet address	0x362b1a3d404f8455813da218339765d6600e0c48
Transaction Hash	0xf5eef5217b460d3a0a89fb98c90a1a0cad69459ff2acbe1500f07897854911d8

Date	8/25/22 20:28
USDT Amount	48,309.26
Sent to wallet address	0x362b1a3d404f8455813da218339765d6600e0c48
Transaction Hash	0xb72de1821faf5109f9e346da594397078f08822058f0c7e04f843ae8384055b5

Date	8/26/22 16:46
USDT Amount	46,666.00
Sent to wallet address	0x362b1a3d404f8455813da218339765d6600e0c48
Transaction Hash	0x5c438d80cb717142cb118eafdd2a3e6e7d88dcf255ac0eae935a7176d6648e61

Date	8/31/22 0:36
USDT Amount	49,095.27
Sent to wallet address	0x362b1a3d404f8455813da218339765d6600e0c48
Transaction Hash	0x232faa344878bc9eb415f58c3bc24e04bb28cd064f5f8055023b23770e9eba9a

Date	9/2/22 11:34
USDT Amount	48,844.74
Sent to wallet address	0x362b1a3d404f8455813da218339765d6600e0c48
Transaction Hash	0x7fa57c47af6f48765415b66b8eab5ec26813ee214b08cf498444c95de9ac7366

Date	9/2/22 20:23
USDT Amount	48,707.77
Sent to wallet address	0x362b1a3d404f8455813da218339765d6600e0c48
Transaction Hash	0xbc9bb054aba765e59f4ccaa89f46f3fc79b7cbca7792cd8b33d527130e766293

Date	9/8/22 1:36
USDT Amount	48,000.00
Sent to wallet address	0x362b1a3d404f8455813da218339765d6600e0c48
Transaction Hash	0xa6be4867c2b2dd94570ee645f7f501e2f0fdea377434be9285733945c42f49b8

Date	9/13/22 2:35
USDT Amount	46,666.00
Sent to wallet address	0x362b1a3d404f8455813da218339765d6600e0c48
Transaction Hash	0xf861f9088c40afba062f834dc1444169a8b5152d77a58ae83798859232d3b9ea

Date	9/15/22 1:28
USDT Amount	34,132.44
Sent to wallet address	0x55df4ecd9066c417103f59d3ecc9b309dedfd131
Transaction Hash	0x75ad8e404670afc0ee8a920b0355acda9c43e4da73054c0720fdffb7a2dc8416

Date	9/15/22 4:26
USDT Amount	14,568.00
Sent to wallet address	0x55df4ecd9066c417103f59d3ecc9b309dedfd131
Transaction Hash	0xc3ab2fc2c1b25934af92ef4584b3dbb5eb4d974da9913fbbc349e412fc7a64ef

Date	9/16/22 21:00
USDT Amount	26,329.00
Sent to wallet address	0x55df4ecd9066c417103f59d3ecc9b309dedfd131
Transaction Hash	0x4e9482d4d4d5dacd396136593bbd88d34e80cca96e35a4b1ecae523fefa3c9ca

Date	9/16/22 21:00
USDT Amount	8,888.00
Sent to wallet address	0x55df4ecd9066c417103f59d3ecc9b309dedfd131
Transaction Hash	0x3dea57d83b98dccb447f871e6358d0e8527e0116c41fae5e3c6c600b2063dcbe

Date	9/20/22 18:39
USDT Amount	48,888.00
Sent to wallet address	0x55df4ecd9066c417103f59d3ecc9b309dedfd131
Transaction Hash	0x3bdf3306d5988cada96e39e3998e9287b1a3e5e72719389911a44ff529037daf

Date	9/20/22 19:47
USDT Amount	8,888.00
Sent to wallet address	0x55df4ecd9066c417103f59d3ecc9b309dedfd131
Transaction Hash	0xce6b015dbf82ef20193daacd8dd08f3f2f2f133bb00d39f52813bb6068b4dbd6

Date	9/21/22 19:14
USDT Amount	57,776.00
Sent to wallet address	0x55df4ecd9066c417103f59d3ecc9b309dedfd131
Transaction Hash	0x5eebab0eeb7526c8b8aaa682fccc39a14867d83db7a6c5d1a3719ebe8208b331

Date	9/23/22 23:25
USDT Amount	57,776.00
Sent to wallet address	0x55df4ecd9066c417103f59d3ecc9b309dedfd131
Transaction Hash	0xc2058ad7177623c8d56175d531daa511d1e15f9c3fd7421075a62135b6fd2fa3

Date	9/24/22 16:34
USDT Amount	26,329.00
Sent to wallet address	0x55df4ecd9066c417103f59d3ecc9b309dedfd131
Transaction Hash	0xf117e59466d1bf73006aace0a0aa5e7c78fcc405f72ac5422fd48badfd2ce882

Date	10/3/22 20:38
USDT Amount	29,829.00
Sent to wallet address	0x55df4ecd9066c417103f59d3ecc9b309dedfd131
Transaction Hash	0xddf434cec3eb69c0c7f331a13ab9992b6f53b4bb0a5fc13cd16877917b5ae8cb

Date	10/5/22 21:39
USDT Amount	26,329.00
Sent to wallet address	0x55df4ecd9066c417103f59d3ecc9b309dedfd131
Transaction Hash	0x5f5baad2dbeb3da93288424893515696433318b90e73180b5aae37e38c049540

Date	10/6/22 13:37
USDT Amount	31,717.00
Sent to wallet address	0x55df4ecd9066c417103f59d3ecc9b309dedfd131
Transaction Hash	0x2a9321912ac85fef6baaa40f261a8df78ae2f31c8c6e202f85f1503aa1480629

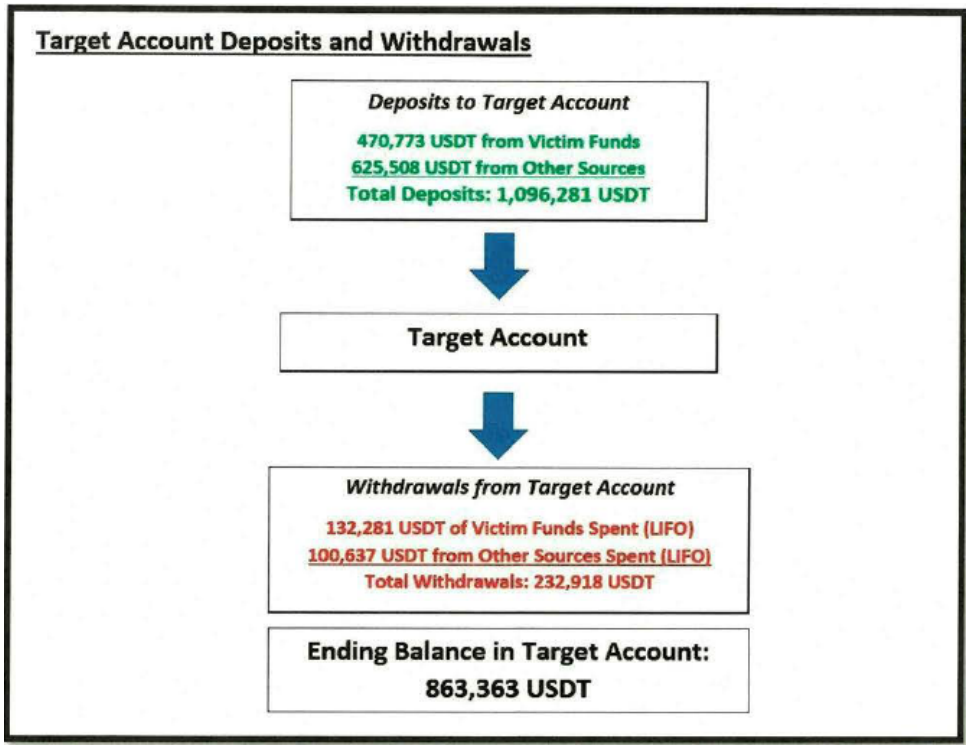
Date	10/6/22 16:50
USDT Amount	52,658.00
Sent to wallet address	0x55df4ecd9066c417103f59d3ecc9b309dedfd131
Transaction Hash	0x02e857c072734b161fdf00baf51a68a141380dfa23f5ba044bc6fecba3d0f23c

52. In total, tracing showed that approximately 1,096,281 USDT—from both Victim 1's funds and other sources[15]—was deposited in VCA d131, though 232,918 USDT was withdrawn from VCA d131. As of the date Tether voluntarily froze the contents of VCA d131 in October 2022, VCA d131 contained 863,363 USDT.[16] Based upon its

15 These other sources include deposits from VCA 91Fc, an address to which Victim 1 had been directed to send funds. Victim 1 reportedly did not send funds to VCA 91Fc.

16 Tether had informed the Federal Bureau of Investigation on October 24, 2022, that it had frozen VCA d131, which currently held a balance of 861,260. However, through its blockchain analysis, the Federal Bureau of Investigation determined that there was a deposit

blockchain analysis, the Federal Bureau of Investigation determined that the contents of VCA d131 at that time are visually summarized as follows:[17]



a. The Federal Bureau of Investigation confirmed that the funds withdrawn from VCA d131 before the address was frozen included 132,281 USDT of Victim 1's funds and 100,637 USDT from other sources, using the last-in, first-out accounting method.

b. The last-in, first-out tracing methodology involves analyzing the flow of tokens moving into and out of a given virtual currency address assuming that the last—or most recent—incoming assets are the first expended or

into VCA d131 on about October 20, 2022, in the amount of 2,103 USDT. It appears that Tether's freeze on the account prevented outgoing transfers from VCA d131 but continued to permit deposits into VCA d131.

17 The Target Account referenced in the visual summary is VCA d131.

sent out.

c. Thus, of the 863,363 USDT present in VCA d131, 338,492 USDT constituted funds transferred from Victim 1's Crypto.com account and 524,871 USDT constituted funds from other sources that had been comingled in VCA d131 with the funds transferred from Victim 1.

53. Given the transfer of 470,773 USDT of Victim 1's funds into VCA d131, and the commingling of Victim 1's funds with other funds transferred into VCA d131, 470,773 USDT of the balance in VCA d131 was identified, conservatively, as subject to seizure and criminal and civil forfeiture. On January 19, 2024, United States Magistrate Judge Karen Frink Wolf issued a Warrant to Seize Property Subject to Forfeiture, authorizing the seizure of "470,773 ERC-20 USDT ASSOCIATED WITH VIRTUAL CURRENCY ADDRESS: 0x55Df4Ecd9066C417103F59d3eCc9B309Dedfd131."[18]

54. Following issuance of the seizure warrant, law enforcement worked with Tether to seize a portion of the funds associated with VCA d131. In summary, Tether used its smart contract(s) to "burn" (*i.e.*, destroy) the USDT tokens associated with VCA d131. Tether then reissued, or "minted," the equivalent amount of new USDT tokens associated with the identified portion of the contents of VCA d131—that is, 470,773 ERC-20 USDT, the Defendant Property—and those tokens were then transferred to a government-controlled wallet.

18 Magistrate Judge Karen Frink Wolf had previously issued a warrant to seize that property on about June 21, 2023. The subsequent warrant was sought to obtain judicial review of the proposed process of transferring the property in the manner described in Attachment A to the Affidavit in Support of Application for Seizure Warrant. That process is described further below.

55. Thereafter, the Defendant Property remained in the custody of the United States government to ensure that access to, or manipulation of, the forfeitable property could not be made absent court order or, if forfeited to the United States, without prior consultation by the United States.

a. The government-controlled wallet to which the Defendant Property was initially transferred was controlled by the Federal Bureau of Investigation, or their designee. The recovery seed for the virtual currency wallet was stored at the Federal Bureau of Investigation office in Chelsea, Massachusetts.

b. In May 2024, the Federal Bureau of Investigation, in coordination with the United States Marshals Service's Complex Assets Unit and Virtual Currency Team, transferred the Defendant Property to a virtual currency wallet controlled by the United States Marshals Service. The Defendant Property has remained in the custody of the United States Marshals Service since that time.

56. The United States is aware that criminals will often incorporate cryptocurrency into their activities due to its potential, and perceived, anonymity and the potential complexity of tracking funds. Criminals will often conduct several transfers of cryptocurrency, convert tokens into other forms of cryptocurrency, and/or comingle unlawfully obtained funds with funds from other sources to conceal and disguise the unlawful source of such funds.

57. Here, by deceiving Victim 1 into transferring funds to both VCA d131 and to VCA 0c48, the perpetrator(s) were able to separate Victim 1's funds and comingle

those proceeds with other funds of unknown origin. In VCA 0c48, Victim 1's funds were comingled with funds from as-yet-unknown sources, and a portion of those commingled funds were then laundered within, and layered into, the deposit to VCA d131. In VCA d131, Victim 1's funds—both directly transferred to that address and indirectly transferred through VCA 0c48—were comingled with additional funds from as-yet-unknown sources in order conceal or disguise the nature, location, and source of Victim 1's funds.

58. Additionally, given the transfer of a portion of Victim 1's funds and other comingled funds from VCA d131 prior to Tether's temporary freeze, VCA d131 appears to be an intermediary wallet. Movement of illicitly obtained funds through VCA d131 would help to conceal and disguise the source of the USDT by layering and severing straight-line connections of blockchain transactions from a victim's account to the perpetrator(s) seeking to eventually convert illicitly obtained cryptocurrencies into fiat currencies.

CLAIM FOR FORFEITURE

59. The allegations contained in paragraphs 1 through 58 of this Verified Complaint are incorporated herein.

60. The defendant in rem is subject to civil forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C). Specifically, 18 U.S.C. § 981(a)(1)(C) authorizes forfeiture of "any property, real or personal, which constitutes or is derived from proceeds traceable to . . . any offense constituting a 'specified unlawful activity' (as defined in [18 U.S.C. § 1956(c)(7)], or a conspiracy to commit such offense." Pursuant to 18 U.S.C. § 1961(1), as incorporated by 18 U.S.C. § 1956(c)(7)(A), violations of 18 U.S.C. § 1343 (relating to wire fraud) are a specified unlawful activity within the meaning of 18

U.S.C. § 981(a)(1)(C). The defendant in rem constitutes, and is derived from, the proceeds of wire fraud and/or wire fraud conspiracy in violation of 18 U.S.C. §§ 1343 and 1349, and is thus subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C).

61. The defendant in rem is subject to civil forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(A). Specifically, 18 U.S.C. § 981(a)(1)(A) authorizes forfeiture of "any property, real or personal, involved in a transaction or attempted transaction in violation of section 1956, 1957, or 1960 of [Title 18], or any property traceable to such property."

a. It is a violation of 18 U.S.C. § 1956(a)(1)(B)(i) to, "knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conduct[] or attempt[] to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity—knowing that the transaction is designed in whole or in part—to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity[.]"

b. It is a violation of 18 U.S.C. § 1957(a), in the circumstances set forth in 18 U.S.C. § 1957(d), to knowingly engage or attempt to engage in a monetary transaction in criminally derived property of a value greater than $10,000 derived from specified unlawful activity.

    i. Pursuant to 18 U.S.C. § 1957(f)(1), a monetary transaction includes "the deposit, withdrawal, transfer, or exchange, in or affecting interstate or foreign commerce, of funds or a monetary instrument . . . by, through, or to a financial institution . . . ."

ii. Pursuant to 18 U.S.C. § 1956(c)(6)(A), a financial institution includes any financial institution as defined in 31 U.S.C. § 5312(a)(2) or regulations promulgated thereunder. Pursuant to 31 U.S.C. § 5312(a)(2)(J), a financial institution includes "a currency exchange, or a business engaged in the exchange of currency, funds, or value that substitutes for currency or funds[.]"

c. It is a violation of 18 U.S.C. § 1956(h) to conspire to commit any offense defined in Section 1956 or Section 1957.

d. The defendant in rem is property involved in money laundering transactions in violation of 18 U.S.C. §§ 1956 and 1957, or is property traceable to such property, and is thus subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A).

PRAYER FOR RELIEF

WHEREFORE, the United States of America requests:

1. that a warrant and summons for arrest of the defendant in rem, in the form submitted with this Verified Complaint, issue to the United States Marshal for the District of Maine, or their designee, commanding them to (i) arrest the defendant in rem, and (ii) give notice to all interested parties to appear and show cause why forfeiture should not be decreed;

2. that judgement of forfeiture be decreed against the defendant in rem;

3. that thereafter, the defendant in rem be disposed of according to law; and

4. that this court grant the United States its costs and all other relief to which the United States may be entitled.

Dated: January 16, 2025

Respectfully submitted,

DARCIE N. MCELWEE
United States Attorney

BY: */s/ Nicholas Heimbach*
Nicholas Heimbach
Assistant United States Attorney
United States Attorney's Office
100 Middle Street
East Tower, 6th Floor
Portland, Maine 04101
(207) 780-3257
Nicholas.heimbach@usdoj.gov

VERIFICATION

I, Kevin McCusker, being duly sworn, depose and state that I am a Special Agent with the Federal Bureau of Investigation and as such have responsibility for the within action, that I have read the foregoing Verified Complaint and know the contents thereof, and declare under penalty of perjury that the contents thereof are true to the best of my knowledge, information, and belief.

The sources of my information and grounds of my belief are official records and files of the United States and information obtained during an investigation of alleged violations of Title 18, United States Code.

Date: January 16, 2025

/s/ Kevin McCusker
Kevin McCusker
Special Agent
Federal Bureau of Investigation

STATE OF MAINE
Cumberland, ss.

Subscribed and sworn to before me this 16th day of January, 2025.

/s/ Kimberley P. Woodward
Kimberley P. Woodward
Notary Public
My commission expires: 11/19/2026