MICHELE BECKWITH
Acting United States Attorney
KEVIN C. KHASIGIAN
Assistant U. S. Attorney
501 I Street, Suite 10-100
Sacramento, CA 95814
Telephone: (916) 554-2700

Attorneys for the United States

IN THE UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, v. APPROXIMATELY 500,001.2 USDT, APPROXIMATELY 1,000,100.145687 USDT, AND APPROXIMATELY 1,285,540.357235 USDT, Defendants.	VERIFIED COMPLAINT FOR FORFEITURE *IN REM*

The United States of America, by and through its undersigned attorney, brings this complaint and alleges as follows in accordance with Supplemental Rule G(2) of the Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions:

NATURE OF ACTION

1. This is a civil action *in rem* to forfeit three amounts of cryptocurrency involved in a sophisticated cryptocurrency fraud scheme that scammed at least a dozen individuals living in cities across the United States out of more than $2.7 million. The perpetrators of this vast fraud scheme persuaded unwitting victims to invest their savings in cryptocurrency platforms called "BIT" and "GLEHFX.com" after being told—falsely—their investments would grow if they simply carried out the

fraudster's investment advice. In truth, the platforms were a farce, and their investment gains were a simulation—manipulated in the platforms to entice further investments and fraud. When the victims recognized the falsity of the investment vehicles, it was too late as their funds had been interdicted by criminals in the investment labyrinth that had been promoted to investors as a safe investment.

2. The cryptocurrency was seized by the U.S. Secret Service ("Secret Service" or "USSS") on or about January 13, 2025, pursuant to Federal seizure warrants, after law enforcement identified several wallet addresses central to the fraud scheme. Law enforcement then traced the stolen cryptocurrency from the facilitating wallet addresses to Tether where it had been converted to USDT, a cryptocurrency stablecoin linked to the U.S. Dollar.

3. The $2.7 million held in three tainted wallet addresses—the "defendant cryptocurrency"—is currently in the custody of the Secret Service and described as follows:

a. Approximately 500,001.2 USDT held in the Tron account **TNihvNZfFYdSjLWyEHiPXQ2u28oXHN1PNu** ("Tron Account 1"),

b. Approximately 1,000,100.145687 USDT held in the Tron account **TTscFqjCSFTpKufe8jjH653JmgYCHvQjdF** ("Tron Account 2"), and

c. Approximately 1,285,540.357235 USDT held in the Ethereum account **0x366e2BEeF3635b644D4698E33Ef557449ABeC8E7** ("Ethereum Account 1").

JURISDICTION AND VENUE

4. This Court has jurisdiction over an action commenced by the United States under 28 U.S.C. § 1345, over an action for forfeiture under 28 U.S.C. § 1355(a).

5. This district is a proper venue pursuant to 28 U.S.C. § 1355 and 28 U.S.C. § 1395 because the acts or omissions giving rise to the forfeiture occurred in this district.

FACTUAL ALLEGATIONS

Cryptocurrency and Virtual Currency Exchanges

6. Virtual currencies are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank like traditional fiat currencies, such as the U.S. Dollar, but are generated and controlled through computer software. Bitcoin ("BTC") is currently the most well-known virtual currency in use.

7. Virtual currency addresses are the virtual locations where currencies are sent and received. Each virtual currency address is controlled using a unique corresponding private key, a cryptographic equivalent of a password needed to access the address. An address is somewhat analogous to a bank account number and is represented as a string of letters and numbers up to 40 characters long. Users can operate multiple addresses at any given time, with the possibility of using a unique address for every transaction. Only the holder of an address's private key can authorize a transfer of virtual currency from that address to another address. Although the identity of an address owner is generally anonymous (unless the owner opts to make the information publicly available), analysis of the blockchain can often be used to identify the owner of a particular address. The analysis can also, in some instances, reveal additional addresses controlled by the same individual or entity.

8. A virtual currency wallet is a software application that interfaces with the virtual currency's specific blockchain and generates and stores a user's addresses and private keys. A virtual currency wallet also allows users to send and receive virtual currencies. Multiple addresses can be stored in a wallet.

9. Many virtual currencies publicly record their transactions on what is known as a "blockchain." The blockchain is essentially a distributed public ledger, run by a decentralized network, containing an immutable and historical record of every transaction utilizing that blockchain's technology. The blockchain can be updated multiple times per hour and records every virtual currency address that ever received that virtual currency. It also maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies.

10. **Stablecoins**: Stablecoins are a type of virtual currency whose value is pegged to a commodity's price, such as gold, or to a fiat currency, such as the U.S. dollar, or to a different virtual currency. For example, USDC and USDT (defined in paragraphs 11 and 14 below) are stablecoins pegged to the U.S. dollar. Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the asset or its derivatives.

11. **Tether (USDT):** Tether Limited ("Tether") is a company that manages the smart contracts (defined in paragraphs 15) and the treasury (*i.e.*, the funds held in reserve) for USD Tether ("USDT")

tokens. USDT is a blockchain-based cryptocurrency whose tokens in circulation are backed by an equivalent amount of U.S. dollars, making it what is known as a "stablecoin." USDT is hosted on the Tron and Ethereum blockchains, among others.

12. **Tron (TRX):** Tron ("TRX") 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 Tron blockchain, which allows anyone to track the movement of TRX and tokens such as USDT.

13. **Ether (ETH) and Ethereum:** Ether ("ETH") is a cryptocurrency that is open source, public, has a blockchain, and is distributed on a network called Ethereum 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 and tokens such as USDT.

14. **USD Coin (USDC):** USD Coin ("USDC") is a blockchain-based stablecoin. USDC is hosted on the Ethereum network, among others. USDC is issued by Centre, a company headquartered in the U.S. USDC is connected to Coinbase and Circle, cryptocurrency exchanges registered in the U.S.

15. **Smart contracts:** 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 blockchain protocols such as Ethereum and Tron to maintain transparency. Multiple cryptocurrencies, including USDT, can utilize the Ethereum or Tron blockchains to take advantage of this technology. Smart contract technology is one of the distinguishing characteristics of Ethereum and Tron and is an important tool for companies or individuals executing trades on these blockchains. 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 or Tron blockchain and is both trackable and irreversible.

16. **Decentralized finance application:** One of the many applications of smart contracts on blockchains such as Ethereum is to facilitate financial transactions involving cryptocurrency that do not rely on a centralized custodial service to execute. Such applications are decentralized in nature as they rely on pre-established smart contracts (rather than trusted intermediaries) to execute code automatically

in response to certain inputs. These applications are commonly used to "swap" virtual currencies, for example, Ethereum for USDT, or USDT for another Ethereum token, such that one asset is sent from the address and an equivalent value (less fees) of the corresponding asset is received into the same address nearly instantaneously, within the same transaction. Services utilizing these mechanisms are often referred to as "decentralized finance applications."

Grass Valley Resident Defrauded of $167,000 in Cryptocurrency

17. This investigation originated with a fraud perpetrated against "RB", a 62-year-old resident of Grass Valley, California, in the Eastern District of California. In June and August 2024, RB was victimized pursuant to an ascending investment fraud scheme known as "Pig Butchering." Pig Butchering originated in China and often begins with a perpetrator sending a victim an unsolicited text message, typically via WhatsApp or a social media/dating website. From the initial message, the perpetrator develops an intimate relationship with the victim using manipulative tactics like those used in online romance scams. Pig Butchering schemes frequently originate in various locations throughout Southeast Asia, including, but not limited to, Hong Kong, Myanmar, Cambodia, Malaysia, Thailand, and Singapore.

18. Pig Butchering victims are referred to as "pigs" because the perpetrators will use elaborate (and often romantic) storylines to "fatten up" victims into believing they are in a trusting relationship. Once the victim reaches a certain level of trust, they are brought into a cryptocurrency investment scheme and provided fabricated evidence to bolster the scheme's legitimacy. Victims are provided fake investment platforms via a website or mobile application that showcases fictious investment gains. The website or application has limited functionality and does not provide the user any access to a cryptocurrency wallet. The perpetrators may also provide fake transaction photos to create the false impression the perpetrators are contributing their own funds to the victim's initial investment. However, the investment gains displayed on the investment platform website or mobile application are fabricated. In truth, the investment platform is a farce.

19. The perpetrator encourages victims to invest more funds into the platform, promising higher returns. Victims can make small initial withdrawals to bolster perceived control over the assets, increasing their trust in the platform and to encourage larger investments. When significant withdrawals

are attempted, however, they are forbidden. Various excuses are given for blocked withdrawals, often involving fees and taxes that are due and sometimes that suspected misconduct created a temporary freeze of the account for compliance purposes. Victims are unable to withdraw their funds regardless of how much additional money is invested. The financial loss causes the victims financial, personal, and emotional ruin and is referred to by the perpetrators as "butchering" or "slaughtering" the victims.

20. The efforts to defraud RB were evident from the perpetrator's initial messages on Facebook because, within weeks, RB was persuaded to purchase USDT, USDC and Bitcoin from two cryptocurrency exchanges and transfer the cryptocurrency to the fraudulent trading application, "BIT" or "BIT App."

21. The "BIT" platform utilized the naming convention of the legitimate cryptocurrency trading business with the same acronym, "BIT." However, the "BIT" application provided to RB was not legitimate, and the allegations herein reference only the illegitimate "BIT" company used to steal from RB. The fake BIT platform deceived RB into believing they achieved huge gains from high-frequency trading. However, the perpetrator offered various excuses—and even demanded more money—when RB attempted to withdraw funds. RB invested approximately $167,000 of cryptocurrency before realizing the investment scheme was a scam.

The "BIT" Fraud Scheme

22. In June 2024, RB received a message from a female named "Linda Gao" while browsing a motorcycle enthusiast Facebook group. Gao claimed to own a motorcycle, and they sporadically chatted on Facebook and on video chats. After a few days of Facebook chats, Gao requested they talk via WhatsApp.

23. RB observed Gao's word usage was abnormal, so he asked Gao if she used a translator. Gao confirmed she did, and RB believes he likely chatted with different people at different times based on Gao's changing personalities, a common tactic deployed by criminal organizations operating in the world of cryptocurrency fraud.

24. Law enforcement believes Gao was a pseudonym or false name and likely a role played by multiple members of the fraud network. After a week or so, RB and Gao's conversations shifted from motorcycles to money and cryptocurrency investing. Gao told RB she became rich by trading

cryptocurrency options and offered to help RB make money trading options. RB confided in Gao that his father had dementia, and he needed money to pay for his father's care.

25. At Gao's direction, RB downloaded the TrustWallet cryptocurrency application and used it to connect to the "BIT" platform via a URL provided by Gao. RB created an account on the BIT platform, accessible via TrustWallet. The BIT platform functioned like a legitimate cryptocurrency platform and displayed customer information such as account numbers, cryptocurrency wallet addresses, investment amounts and gains, and deposit/withdrawal functions. The BIT app featured graphics and layouts consistent with many smartphone currency trading applications.

26. Unlike legitimate trading websites, the BIT website's URL changed each month. When RB joined the platform, the URL was https://cntzcy.com, but in late July 2024, RB received an email from the platform stating that due to a "hacked malicious attack," the web platform's domain changed to https://cdsslt.com. In late August 2024, RB received another email from the platform stating the platform's web domain had changed again, this time to https://oluarr.com, due to yet another "hacked malicious attack." The frequent domain change is a hallmark of bogus websites, allowing the site to continue their criminal operations when victim reporting results in the domain's identification as fraudulent.

27. Gao showed RB how to use BIT and explained the different tiers of investment, expected rate of return from the various investment pool options (e.g., the 30-second pool, 60-second pool, or 90-second pool), and that by investing more, higher rates of return were likely.

28. In mid-July 2024, RB transferred his existing cryptocurrency holdings at Crypto.com to BIT. RB transferred 38,150 USDC from his Crypto.com account to his BIT account. RB had a troublesome history with Crypto.com, experiencing repeated disruptions in service, and Gao urged RB to instead use the Strike exchange. RB also transferred $5,000 from his Bank of America account to his Strike account, where he purchased $5,000 of BTC and then sent the $5,000 BTC to BIT. At the completion of RB's conversion from Crypto.com to Strike, RB had a $60,000 balance in his BIT account. In mid-August 2024, RB successfully withdrew $60,000 from his BIT account, ultimately transferring that amount to his Bank of America account, an experience that convinced RB that Gao's investment

opportunity was sincere. RB believed if Gao planned to steal his $60,000, they would not have allowed him to withdraw the funds.

29. Gao offered to "loan" RB $50,000 to elevate him into a higher tier on BIT. RB agreed to the loan and RB's balance on BIT displayed a $50,000 increase. Gao later "loaned" RB another $150,000, and RB's BIT balance reflected the $150,000 infusion from Gao. Gao ultimately convinced RB to deposit another $160,000 to elevate into the next investment tier. RB complied and invested the $160,000; his new account balance—together with the "loans," RB's previous investments, and the purported gains—was sufficient to reach the next investing tier.

30. To complete the $160,000 investment, RB wired $160,000 from his Bank of America account to his Strike account and purchased 2.69292824 BTC. RB then transferred the 2.69292824 BTC to his BIT account. At this time, in late August 2024, RB's BIT account showed a 924,000 USDT balance. In mid- to late-August 2024, RB attempted to withdraw approximately 674,000 USDT from BIT, but the withdrawal stalled and the platform displayed the messages "pending clearance" or "on hold."

31. On August 21, 2024, RB was told to "contact customer service"—and from that conversation RB learned his account was frozen for "wrong inputs of a receiving address," but RB confirmed he had entered the correct address into BIT. RB then contacted BIT's online representatives, who told RB to deposit 20% of his balance (approximately $180,000) to unfreeze the funds held at BIT. If RB refused to deposit the additional $180,000 within three days, his account balance would be donated to the United Way. Based on the demand for more money, RB concluded the BIT investment was a scam and contacted law enforcement.

Common "Fraud" Cryptocurrency Addresses and More BIT Scam Victims

32. BIT utilized a series of shared cryptocurrency addresses to target victims and move certain categories of cryptocurrency, such as Bitcoin and Ethereum. In the scheme to defraud RB, the scammers utilized shared wallet addresses to receive and transfer RB's (and other victims') stolen funds. The shared cryptocurrency addresses used to defraud RB are reproduced below:

a. For BTC:

Addresses **19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV**, **13AVd6XBaPxTzDoPRht6VpNw2NT3BWVoPT**, **bc1qjh6dc0scfu9vdyf2yjdhj96uvlvtf6tdhhw8ml**, and **19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV** RB made several deposits.

b. For Ethereum:

Address **0xE073907d67A125DB8Fac7ea4719B3AaB94752D03**. RB made two USDC deposits to this address.

Address **0xC46ABF247b6a0d86FF178561D0893ddD0f00C23e** was provided to RB for USDT and USDC deposits.

Address **0xE6626588bAea62C2229783D082d362c9525a1296** was provided for USDT deposits.

e. For Tron:

Address **TJTWrPyts7ahu22iWupAfeGKDojqy9nLFF** was provided for USDT deposits on the Tron network.

33. Law enforcement connected these wallet addresses to victim complaints on the Federal Bureau of Investigation's ("FBI") Internet Crime Complaint Center, known as IC3 (http://www.ic3.gov). The following IC3 reports identify seven additional victims of similar Pig Butchering scams that used identical wallet addresses or websites to defraud many individuals:

a. WS, a resident of Lillington, North Carolina, reported losing $23,468 worth of cryptocurrency in 2024 after sending Bitcoin to the address **19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV** used by BIT and the URL https://cdsslt.com.

b. PT, a resident of Forsyth, Georgia, reported losing $85,200 in 2024 after sending USDT to **0x211d18f4262383911500e1298e02c4865e91abe2** on a platform using the web domain Bit-world.cc. The USDT was forwarded from that address to **0xE073907d67A125DB8Fac7ea4719B3AaB94752D03**.

c. TM, a resident of Roebuck, South Carolina, reported being defrauded of $2,000 in cryptocurrency in July 2024 having lost at least $2,000 in cryptocurrency on the BIT platform with the URL OLUARR.com.

d. MW, a resident of Concord, North Carolina, lost $50,000 to a scam in September 2024 on the BIT platform after meeting a woman on a motorcycle enthusiast Facebook group.

e. RJ, a resident of Bellevue, Pennsylvania, reported having lost $50,000 worth of cryptocurrency in April 2024 after sending funds to Ethereum address **0xaf25c5a45115F523049F7fc05D4BAD22c60e2F34** on the BIT platform with the domain bwdcoin.cc.

f. MN, a resident of the Czech Republic, lost $45,000 of cryptocurrency in 2024 via wallet address **0xaf25c5a45115F523049F7fc05D4BAD22c60e2F34** on a website with the domain bit-world.cc.

34. Using the Blockchain, law enforcement identified several more victims who transferred BTC to the wallet addresses from RB's fraud scam and the seven victims identified from the FBI's IC3 network. These victims, identified via the Blockchain based on wallet addresses used to defraud U.S. citizens, transferred a total of 19.55870079 BTC, worth approximately $1,173,647:

a. Minneola, Florida resident GF sent 2.95221562 BTC (worth approximately $191,024) to **19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV** in July 2024. GF reported to law enforcement that he was convinced by an online personality to wire $741,769 from his Chase and Wells Fargo accounts to Coinbase but was now unable to withdraw the funds from what appeared to be a "fake portal."

b. North Logan, Utah resident KD sent 0.82139442 BTC (worth approximately $48,950) to **13AVd6XBaPxTzDoPRht6VpNw2NT3BWVoPT** in August 2024. KD reported losing at least $200,000 invested on the BIT platform with the URL OLUARR.com, the same URL used to defraud RB.

c. Jacksonville, FL resident AB sent 2.37151095 BTC (worth approximately $137,574) to **19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV** in August 2024. AB had invested $348,000 via Crypto.com after he learned of an investment opportunity from someone he met in a chatroom.

d. U.S. resident RS sent a total of 0.61050823 BTC (worth approximately $39,493) to **19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV** on July 16, 2024.

e. U.S. resident DS sent a total of 3.28287845 BTC (worth approximately $199,716) to **19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV** on August 9, 2024.

f. U.S. resident JK sent a total of 0.21805695 BTC (worth approximately $12,821) to **19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV** on August 12, 2024.

g. U.S. resident JS was defrauded of 6.60996847 BTC (worth approximately $385,073) after sending the BTC to **19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV** and **13AVd6XBaPxTzDoPRht6VpNw2NT3BWVoPT** in June and August 2024.

The fraud victims and their losses described in paragraphs 34 and 35 are summarized as follows:

Name	City/State/Country	Loss	Address(es)
RB	Grass Valley, CA	$167,000	19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV 13AVd6XBaPxTzDoPRht6VpNw2NT3BWVoPT 0xE073907d67A125DB8Fac7ea4719B3AaB94752D03 0xC46ABF247b6a0d86FF178561D0893ddD0f00C23e 0xE6626588bAea62C2229783D082d362c9525a1296 TJTWrPyts7ahu22iWupAfeGKDojqy9nLFF
WS	Lillington, NC	$23,468	19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV
PT	Forsyth, GA	$85,200	0x211d18f4262383911500e1298e02c4865e91abe2

TM	Roebuck, SC	$2,000	Unknown
MW	Concord, SC	$50,000	Unknown
RJ	Bellevue, PA	$50,000	0xaf25c5a45115F523049F7fc05D4BAD22c60e2F34
MN	Czech Republic	$45,000	0xaf25c5a45115F523049F7fc05D4BAD22c60e2F34
GF	Minneola, FL	$191,024	19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV
KD	North Logan, UT	$200,000	13AVd6XBaPxTzDoPRht6VpNw2NT3BWVoPT
AB	Jacksonville, FL	$348,000	19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV
RS	United States	$39,403	19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV
DS	United States	$199,716	19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV
JK	United States	$12,821	19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV
JS	United States	$385,073	19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV 13AVd6XBaPxTzDoPRht6VpNw2NT3BWVoPT
Total		**$1,798,705**	

Seizure of Tron Accounts 1 and 2

35. Law enforcement traced victim funds through a series of momentary transfers, known as "hops," to Tron Accounts 1 and 2 at Tether. The fraudulent "hops" involving Tron Account 1 are described below.

a. RB transferred 2.6921677 BTC (approximately USD value $158,996.20) on August 16, 2024, to Bitcoin address **19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV**. Twelve minutes later, the 2.6921677 BTC "hopped" to address **1AD61wBMvt5DRPRV5mG6zAmpT91TGdDrqy**, an address controlled by the cryptocurrency exchange ChainUp and used as a unique customer deposit address.

b. ChainUp records reveal that one minute after the 2.6921677 BTC was deposited into **1AD61wBMvt5DRPRV5mG6zAmpT91TGdDrqy**, someone attempted to exchange the 2.6921677 BTC for USDT. The initial exchange was blocked, but a second attempt two minutes later successfully swapped the 2.6921677 BTC for 158,961.393 USDT, a purposeful conversion to obfuscate the nature, source, ownership, control, and source of funds.

c. Nineteen minutes after the swap from BTC to 158,961.393 USDT, someone moved 158,642.4703 USDT to wallet address **TQQRqSbWvoQBDixpZpCUnW8PpZiAbWmqHL**. There was no other activity in the account between the deposit of the BTC, the exchange for USDT, and the withdrawal of USDT.

36. On August 21, 2024, the 158,642.47 USDT and an additional 450,000 USDT transferred into the account over the ensuing three days, moved to address **TCQBkjYHqx6HV2FG2PF2mWor2tULJTa9ae**. Over the next day, 50,000 USDT was withdrawn, 370,000 USDT was deposited, and then 500,000 USDT moved to Tron Account 1, where it was frozen by Tether and then seized by law enforcement based on its involvement in the BIT investment scam.

37. On August 21, 2024, 1,600,003 USDT was deposited into Tron Account 2, funds that originated from wallet addresses central to the BIT scam. The 1,600,003 USDT involved two large deposits: one input of 300,003 USDT (segment 1 of 2), and another input of 1,300,000 USDT (segment 2 of 2).

38. Each segment involved cryptocurrency (USDC, USDT, and BTC) transferred from BIT-involved (and compromised) wallet addresses to ChainUp Account 1, where, like Tron Account 1, the stolen funds were immediately swapped for USDT to obscure their involvement in the fraudulent scheme.

a. The 300,000 USDT segment originated from addresses attributed to the BIT scam in the form of BTC and USDC sent from compromised wallet addresses to ChainUp Account 1, where the funds were swapped for USDT. The funds "hopped" across several wallet addresses, comingling with a small amount of other cryptocurrency, and then deposited into Tron Account 2. Approximately 300,000 USDT of that deposit is traceable to wallet addresses attributed to victims of the BIT scam.

b. The 1,300,000 USDT segment originated in from addresses attributed to the BIT scam. The movement of funds occurred in two paths. In one path, an account at another cryptocurrency exchange, 100ex Account 1 received deposits of USDC and USDT (through either one or two hops) from an address attributed to the BIT scam. 100ex Account 1 swapped the USDC for USDT and transferred the USDT to 100ex Account 2, where 320,554 USDT of the transferred assets were traceable to addresses attributed to the BIT scam.

c. In a second path, USDC, ETH, and BTC were sent from addresses attributed to the BIT scam directly to ChainUp Account 1 and then swapped for USDT. The USDT was then

sent to wallet address **TQQRqSbWvoQBDixpZpCUnW8PpZiAbWmqHL** and transferred to 100ex Account 2, where approximately 235,320 USDT of the transferred assets were traceable to addresses attributed to the BIT scam.

39. On June 30, 2024, withdrawals of 500,001 USDT and 775,595 USDT were made from 100ex Account 2 and then transferred to wallet address **TCQBkjYHqx6HV2FG2PF2mWor2tULJTa9ae** where the funds were commingled with segment 1 and then transferred to Tron Account 2, where it was frozen by Tether and then seized by law enforcement based on its involvement in the BIT investment scam. At the time the accounts were frozen, the USDT balances were 500,000 USDT in Tron Account 1 and 900,000.145687 USDT in Tron Account 2.

40. Additional transactions occurred within Tron Accounts 1 and 2 after they were frozen by Tether in early September 2024. In Tron Account 1, no transactions had previously occurred other than the 500,000 USDT transfer. However, on September 10, 2024, while the account was frozen, approximately 70 TRX—Tether's native coin—was deposited into the account. Later the same day, an unknown user attempted a USDT transaction but failed, and a series of additional USDT transaction attempts followed. Similar USDT transactions occurred in Tron Account 2, but they also failed. This behavior is consistent with someone attempting to withdraw USDT from the account and then learning Tether blocked the withdrawals.

41. On September 11, 2024, Tether informed law enforcement that someone using the name "linda" contacted Tether from the email address "linda11661166[@]gmail.com" claiming ownership of both addresses for Tron Account 1 and Tron Account 2. Law enforcement recognized the name "Linda" as the name used by the person who led RB to invest on the BIT platform.

42. On September 17, 2024 at 3:31 PM, law enforcement received an email from "linda11661166[@]gmail.com" stating, "TNihvNZfFYdSjLWyEHiPXQ2u28oXHN1PNu [sic] This is my address and I would like to know how I can get my funds unfrozen and be able to transfer my assets normally, thank you." The **TNihvNZfFYdSjLWyEHiPXQ2u28oXHN1PNu** wallet address is Tron Account 1.

43. Three minutes after the email from "linda11661166[@]gmail.com," law enforcement received an email from "zjing6950[@]gmail.com" stating, "TTscFqjCSFTpKufe8jjH653JmgYCHvQjdF [sic] This is my address and I would like to know how I can get my funds unfrozen and be able to transfer my assets normally, thank you." The **TTscFqjCSFTpKufe8jjH653JmgYCHvQjdF** wallet address is Tron Account 2.

44. Law enforcement observed similar language used in the two emails, and the first email was sent from an address claiming ownership of both addresses. Law enforcement has since received several emails from other email addresses claiming ownership of one or both Tron Accounts.

45. To verify each requesting party's ownership claim, law enforcement asked each party to screen shot or take a video of them operating the wallet. One individual responded with a video that appeared to show a recording of a mobile phone with a Chinese language interface being used to access a wallet controlling Tron Account 2.

46. Law enforcement replied to that user seeking their location to host an in-person meeting. No one responded for over one month, until late December 2024, when a user responded and demanded law enforcement remove all restrictions on the address—this individual claimed to be "from China and currently in Hong Kong." Law enforcement replied with a request to find a mutually agreeable location to discuss the origin of the funds. As the filing of this complaint, the user has not replied to law enforcement.

Laundering Fraud Proceeds Using Tron Accounts 1 and 2

47. Using public blockchains and records obtained from cryptocurrency exchanges law enforcement used a "last in, first out" (or "LIFO") tracing methodology, in which the cryptocurrencies from immediately preceding transfers are the first withdrawn in subsequent transfers before any other funds, to examine the source of the USDT received by Tron Accounts 1 and 2.

48. The analysis focused on identifying the source of all significant USDT deposits into the accounts (excluding *de minimis* amounts, specifically one deposit each of 1.20 USDT, 1.00001 USDT, and 100 USDT), including those USDT assets that remain frozen after other assets were withdrawn.

49. The tracing showed that large amounts of Bitcoin, ETH, USDT, and USDC cryptocurrency moved from the addresses tied to the BIT scam using some combination of sequencing

hops and decentralized swaps on the blockchain, rapid "pass-through" movement through exchange accounts without converting to a different cryptocurrency or network, rapid "pass-through" movement through exchange accounts with conversion to a different cryptocurrency or network, the use of more than one exchange in sequence, re-aggregation after the movement through exchange accounts, and culminating in transfers to Tron Accounts 1 and 2.

50. During this investigation, law enforcement reviewed records from cryptocurrency exchanges ChainUp and 100ex, which establish that most of the funds in Tron Accounts 1 and 2 originated from BIT victims. Customer due diligence records indicate the accountholders were from the People's Republic of China, and the background of their photographs appear to have been taken in the same corner of the same room. In two of the photos, the same mark appears on a background wall. Further, the account transactions are nearly identical (deposits of BTC, ETH, USDC and USDT with assets swapped to USDT on the Tron network) and withdrawals from the ChainUp accounts were to the same wallet addresses, indicating the same organization used the ChainUp and 100ex accounts to launder of the proceeds of cryptocurrency fraud.

GLEHFX.com Fraud Scheme

51. During the BIT scam investigation, law enforcement learned of another victim, a 38-year-old resident of San Jose referred to as "RM," who reported a fraud similar to the BIT scheme that defrauded RB of $167,000:

a. RM was involved in the scam during the same time period as RB;

b. RM met an Asian woman online who claimed to reside in a city on the West Coast;

c. The fraudster corresponded with RM using Facebook messaging and video chat;

d. The fraudster used the pretext of their relationship to introduce RM to a speculative short-term trading opportunity in cryptocurrency utilizing a web site and a decentralized wallet application;

e. The fraudster claimed to be advised by an uncle who was a successful trader and led RM to falsely believe they added funds to his account;

f. RM funded the investments with cryptocurrency purchased on an exchange—only after being coached through the process of creating the exchange account and wiring funds from his traditional bank accounts;

g. RM was led to believe that his investments had grown substantially in value; and,

h. RM was led to believe that his account had been frozen and he had to pay a substantial fee to access his funds before realizing he was being defrauded.

52. In June 2024, RM connected with an individual named "Chen Yue" on Tinder. They began an online relationship and communicated on WhatsApp and Line. RM described Yue as an attractive Chinese female who spoke fair English but was neither fluent nor a native English speaker. She appeared to live in an apartment and claimed to reside in the hills of Los Angeles, although RM was not provided any proof that she lived in Los Angeles. RM said that sometimes their conversations abruptly ended because what appeared to be a servant entered the room where she was video chatting.

53. In July 2024, Yue encouraged RM to begin investing in an online application associated with a webpage known as "GLEHFX.com." The application and webpage purport to make their users money through short-term leveraged short-selling gold contracts. RM funded the gold trading account with payments of ETH. Yue guided him through the process of opening a Kraken account and RM funded his Kraken account with transfers from his Bank of America and Wells Fargo accounts.

54. Prior to interacting with this website, RM had little knowledge and no experience in trading cryptocurrency. Yue said that she was being advised by a rich uncle who was successful in gold trading. RM believed that Yue had also added $85,000 into the account. In August 2024, RM made four deposits from his Kraken account to the GLEHFX.com application totaling 42.143 ETH, which at the time of the transactions had a value of $109,556.

55. Similar to the BIT scam, GLEHFX.com account gave the false impression that RM's investment made a $480,000 profit in just a few weeks. After RM told Yue that he had no additional money to invest and wanted to withdraw his profits, the website's account administrator informed RM that he was suspected of money laundering. The administrator told RM he had to deposit an additional $85,000 "to lift the account," and only then would his money be returned. RM became suspicious and questioned Yue. RM drove to a residential address in San Jose that Yue told RM that she owned as an investment property, but the residents at the address had never heard of Yue. At that point RM realized he had been defrauded and reported the fraud to law enforcement.

56. Law enforcement used the Blockchain to trace RM's funds from the wallet addresses used on GLEHFX.com, through a series of transfers across cryptocurrency addresses and then to their deposit in ETH Account 1.

57. RM invested in the GLEHFX.com application by transferring ETH from his Kraken account to the Ethereum address **0x899542876793412ba19D0b3265D01cea8F9E129a**, a wallet address provided to him by Yue. From there—wallet address ending in **9E129a**—the funds moved to a wallet address beginning with **0x97e6**, where they were aggregated with other funds and moved to wallet address **0xaC319FBA26610b7685Cb2563D00Ef99f51A7553f**, a wallet address connected to a series of similar "Pig Butchering" scams across the United States:

a. A resident of Clearwater, Florida reported a loss of $30,000 of cryptocurrency in May 2024. The victim reported a woman he met online directed him to open an account with a site called "Golden Elephant" and he sent $30,000 worth of cryptocurrency to the address **0x6ADb699b26e77F470a8F2bE0298957C4f2290A35**. He was later unable to withdraw his funds and realized it was a fraud scam.

b. A resident of San Francisco, California reported losing $25,000 in a cryptocurrency scam in October 2024. The victim reported that a woman he met through a wrong number call convinced him to invest his cryptocurrency in a site accessed through an iPhone application called "sdcfskdvt." At the suspect's direction, he sent cryptocurrency to the wallet address **0xc296E0E97b4E17d213df2BC044BE356C0499a332**. He later realized he was defrauded when he could not withdraw any funds and deposits that were purportedly made by the fraudster to the victim's account did not appear on the Blockchain.

c. A resident of Reno, Nevada reported a theft of $118,400 in cryptocurrency in March 2024. The victim reported that he was befriended by a female he met through a wrong number text message. She convinced him to take out a loan and invest through a web site using the URL DMMtopbitus.com. The victim sent the funds to the Ethereum address **0x7255E1fba48783d1AD5f8b7af1ceB0621d67AD86** at the direction of the suspect and learned it was a scam after he could not withdraw his funds.

d. A resident of Leander, Texas reported a fraud of $46,000 in early 2024. The victim reported being befriended by a female he met through a wrong number text message. The woman convinced the victim to invest in a website at the address DMMtopbitus.com, and he deposited $46,000 in ETH to the wallet address **0x7255E1fba48783d1AD5f8b7af1ceB0621d67AD86** before realizing it was a scam after being asked to prepay his taxes.

e. A resident of McDonough, Georgia reported as loss of $133,580 that occurred on or about June 21, 2024. The victim reported having sent cryptocurrency to a fraudulent platform named DMM Bitcoin, at the direction of a friend he met through a messaging app. The victim was directed to send ETH to the address

0x1D95B2286cC4E8046bb868A1F20b2EC7CcafaB9F. The victim later realized this was a scam.

In total, these six victims reported losses of $462,536.

Name	City/State/Country	Loss	Address(es)
RM	San Jose, CA	$109,556	0x899542876793412ba19D0b3265D01cea8F9E129a
O-1	Clearwater, FL	$30,000	0x6ADb699b26e77F470a8F2bE0298957C4f2290A35
O-2	San Francisco, CA	$25,000	0xc296E0E97b4E17d213df2BC044BE356C0499a332
O-3	Reno, NV	$118,400	0x7255E1fba48783d1AD5f8b7af1ceB0621d67AD86
O-4	Leander, TX	$46,000	0x7255E1fba48783d1AD5f8b7af1ceB0621d67AD86
O-5	McDonough, GA	$133,580	0x1D95B2286cC4E8046bb868A1F20b2EC7CcafaB9F
Total		**$462,536**	

58. The proceeds from the above fraud scams were transferred to the wallet address **0xaC319FBA26610b7685Cb2563D00Ef99f51A7553f**, the same wallet involved in RM's fraud, as well as the victim in San Francisco who invested $25,000. In October 2024, approximately 292.8355 ETH was moved from **0xaC319FBA26610b7685Cb2563D00Ef99f51A7553f** to wallet address **0x366e2BEeF3635b644D4698E33Ef557449ABeC8E7** ("Ethereum Account 1")—at this time, the only cryptocurrency in the wallet was the 292.8355 ETH. In mid-November 2024, approximately 92 ETH was converted to approximately 285,157.35 USDT, at which time Tether froze the account. When Tether froze the account, the USDT balance in Ethereum Account 1 was approximately 281,158 USDT.

59. On November 20, 2024, while Ethereum Account 1 was in the process of being frozen, someone withdrew nearly all the USDT in the account, leaving a USDT balance of just 0.547356 USDT. However, the Ethereum wallet address containing the remaining USDT still contained a substantial amount of ETH traceable to the tainted wallet addresses. The Ethereum account remained frozen by Tether and therefore could receive new deposits of USDT, but not withdrawals.

60. On December 1, 2024, Ethereum Account 1 converted 348.8 ETH to 1,285,539.809879 USDT, allowable transactions during the freeze. On December 26, 2024, Tether informed law enforcement they had been contacted by someone claiming ownership of Ethereum Account 1. This individual went by the name "rui" and the email address from "163.com." Tether provided "rui" with contact information for law enforcement, but "rui" did not contact law enforcement.

61. Law enforcement used the Blockchain to trace the funds deposited into Ethereum Account 1 and concluded that all of the USDT deposited into Ethereum Account 1 was derived from ETH deposits into the account and then swapped within the account for USDT using a decentralized finance application.

62. There were three deposits of ETH into the account:

a. A deposit of 0.1 ETH on October 13, 2024,

b A deposit of 292.735563 ETH on October 13, 2024, and

c. A deposit of 147.588713 ETH on November 28, 2024.

63. All of the ETH received by Ethereum Account 1 originated from six "funnel accounts," which collected ETH from several sources and forwarded via either one or two "hops" to Ethereum Account 1. The Blockchain reveals that most of the "funnel accounts" connected to Ethereum Account 1 were identified by victims as scam deposit addresses.

64. As explained above, criminals engaged in cryptocurrency frauds often conduct otherwise unnecessary transactions in an effort to layer ill-gotten funds to ultimately conceal or disguise the nature, location, source, ownership, or control of those proceeds. The aggregation of illicit funds in "funnel accounts" and then forwarding the funds through one or more hops to an aggregation address where the funds are converted to another type of cryptocurrency reveals an intent to conceal and disguise the nature, location, source, and ownership of the fraud proceeds.

65. On January 13, 2025, law enforcement seized Tron Account 1, Tron Account 2, and Ethereum Account 1 based on a finding of probable cause by the Honorable U.S. Magistrate Judge Carolyn K. Delaney, Chief Magistrate Judge of the United States Court for the Eastern District of California, Case Nos. 2:25-sw-0030-CKD, 2:25-sw-0031-CKD, and 2:25-sw-0032-CKD.

FIRST CLAIM FOR RELIEF
18 U.S.C. § 981(a)(1)(C)

66. The above paragraphs are incorporated by reference as though fully set forth herein.

67. The United States alleges that the defendant cryptocurrency was derived from proceeds traceable to an offense constituting a "specified unlawful activity" as defined in 18 U.S.C. § 1956(c)(7), which incorporates the definition of "specified unlawful activity" found in 18 U.S.C. § 1961(1) and is

therefore subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C). Wire Fraud in violation of 18 U.S.C. § 1343, constitutes "specified unlawful activity" as defined in § 1961(1).

SECOND CLAIM FOR RELIEF
18 U.S.C. § 981(a)(1)(A)

68. The above paragraphs are incorporated by reference as though fully set forth herein.

69. The defendant cryptocurrency is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(A) because it was involved in a transaction or attempted transaction in violation of sections 1956 and 1957 of Title 18, an offense punishable by more than one year's imprisonment.

PRAYER FOR RELIEF

WHEREFORE, the United States prays that:

1. Process issue according to the procedures of this Court in cases of actions *in rem;*

2. Any person having an interest in said defendant cryptocurrency be given notice to file a claim and to answer the complaint;

3. The Court enter a judgment of forfeiture of the defendant cryptocurrency to the United States; and

4. The Court grant such other relief as may be proper.

DATED: 6/12/2025

MICHELE BECKWITH
Acting United States Attorney

By: /s/ Kevin C. Khasigian
KEVIN C. KHASIGIAN
Assistant U.S. Attorney

VERIFICATION

I, David Berry, hereby verify and declare under penalty of perjury that I am a Special Deputy U.S. Marshal with the U.S. Secret Service Cyber Fraud Task Force and a Criminal Investigator with Santa Clara County Office of the District Attorney, that I have read the foregoing Verified Complaint for Forfeiture *In Rem* and know the contents thereof, and that the matters contained in the Verified Complaint are true to the best of my knowledge and belief.

The sources of my knowledge and information and the grounds of my belief are official files and records of the United States, information supplied to me by other law enforcement officers, as well as my investigation of this case, together with others, as a Special Deputy U.S. Marshal with the United States Secret Service.

I hereby verify and declare under penalty of perjury that the foregoing is true and correct.

Dated: June 12, 2025

/s/ David Berry
DAVID BERRY
Criminal Investigator, Santa Clara County
Office of the District Attorney
Special Deputy U.S. Marshal,
U.S. Secret Service Cyber Fraud Task Force

(Signature retained by attorney)