IN THE DISTRICT COURT OF THE UNITED STATES
FOR THE DISTRICT OF SOUTH CAROLINA
GREENVILLE DIVISION

UNITED STATES OF AMERICA, Plaintiff, vs. 50,471.58 TETHER CRYPTO CURRENCY (USDT), Defendant *in Rem*.	)	CIVIL ACTION NO.:

UNITED STATES' COMPLAINT FOR FORFEITURE *IN REM*

The Plaintiff, United States of America, brings this complaint and alleges as follows, in accordance with Rule G(2) of the Supplemental Rules for Admiralty and Maritime Claims and Asset Forfeiture Actions.

NATURE OF THE ACTION

1. This is a civil action *in rem* to forfeit to the United States of America funds in the amount of 50,471.58 Tether Crypto Currency ("USDT") ("Defendant Funds"), pursuant to 18 U.S.C. § 981(a)(1)(A) and 18 U.S.C. § 981(a)(1)(C). The United States seeks forfeiture based upon a reasonable belief that the Government will be able to meet its burden of proof at trial to show that the Defendant Funds constitutes, or is traceable to:

a. property involved in wire fraud transactions or attempted wire fraud transactions in violation of 18 U.S.C. § 1343;

b. property involved in money laundering transactions or attempted transactions in violation of 18 U.S.C. § 1956(a)(1)(A)(i), and/or § 1956(a)(1)(B)(i) and/or 1957;

c. property involved in an illegal money transmitting business, in violation of 18 U.S.C. § 1960; and/or

d. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(c)(7) and;

e. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(h) and;

f. property involved in money transactions in criminally derived property or attempted money transactions, in violation of 18 U.S.C. § 1957.

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction over an action commenced by the United States pursuant to 28 U.S.C. § 1345, and over an action for forfeiture by virtue of 28 U.S.C. § 1355. This Court has *in rem* jurisdiction over the Defendant Funds pursuant to:

(a) 28 U.S.C. § 1355(b)(1)(A), because acts or omissions giving rise to the forfeiture occurred in the District of South Carolina; and

(b) 28 U.S.C. § 1355(b)(1)(B), because venue properly lies in this district pursuant to 28 U.S.C. § 1395.

THE DEFENDANT *IN REM*

3. The Defendant Funds consists of 50,471.58 USDT valued at approximately $50,474.35 in United States Currency, obtained by agents with the United States Secret Service ("USSS") during an investigation into a transnational criminal organization running an exploitation of elderly and social engineering scam. The funds were seized from a cryptocurrency custodial wallet under the control of Binance, identified by account number xxxxx2276 (the "Subject Account") and under the name of Guo Baokun (as google translated from 郭宝昆)("GUO").

4. The USSS seized the 50,471.58 USDT, for federal forfeiture. The Defendant Funds are currently restrained and pending deposit to an account under the control of United States Secret Service.

5. In accordance with the provisions of 19 U.S.C. § 1606, the Defendant Funds have a total domestic value of approximately $50,474.35 in United States Currency.

KNOWN POTENTIAL CLAIMANTS

6. The known individual whose interests may be affected by this litigation are:

   a. Guo Baokun who may have an interest in the Defendant Funds because he was the named account holder of the account seized by USSS during this investigation.

BASIS FOR FORFEITURE

7. Pursuant to the pleading requirements of Supplemental Rule G(2)(f), Plaintiff alleges that there is a factual basis to support a reasonable belief that the Government will

be able to meet its burden of proof at trial to show that the Defendant Funds are subject to forfeiture to the United States, based in part upon the following:

a. USSS and local law enforcement agencies were investigating a transnational criminal organization running an exploitation of elderly and social engineering scam. In summary, investigating agents determined that a scamming group has been using social engineering to contact elderly individuals and convince them that their bank accounts are compromised. Once the scammers have engagement from the victim, they instruct them that their bank accounts are compromised and that they need to put their funds in a secure location while they investigate. The victims then withdraw their funds in cash and take it to a BTC Automated Teller Machine ("ATM"). From that ATM, the funds are sent to a cryptocurrency wallet address provided by the suspects.

b. Digital currency (also known as virtual currency or cryptocurrency)[1] is generally defined as an electronic-sourced unit of value that can be used as a substitute for fiat currency (i.e., currency created and regulated by a government). Digital currencies exhibit properties similar to other currencies, but do not have a physical form, existing entirely on the internet. Digital currency is not issued by any government or bank (in contrast with fiat or conventional currencies) and is instead generated and controlled through computer software operating on a

[1] For purposes of this complaint, the terms "digital currency," "cryptocurrency," and "virtual currency" are used interchangeably and address the same concept.

decentralized peer-to-peer network, often referred to as the blockchain or public ledger. Digital currency is legal in the United States and accepted for legitimate financial transactions. However, digital currency is often used for conducting illegal transactions or for concealing or disguising the true nature, source, location, ownership, or control of illegally obtained proceeds. Bitcoin ("BTC") is one of the most commonly used and well-known digital currencies. Ethereum ("ETH") is another popular and commonly used digital currency.

c. A stablecoin is a digital currency whose market value is attached to or "pegged" to another stable asset. Differing from normal digital currencies, the value of stablecoins are pegged to assets such as fiat currencies like the United States Dollar ("USD") or the Euro, or other types of assets like precious metals or other digital currencies. Stablecoins are thus used to mitigate the volatility in the price of digital currency by mimicking the value of a fiat currency, without converting digital currency into fiat. While there are various legitimate uses for stablecoins, they are popular with cyber-criminals who seek to hold digital currency proceeds of crime at a stable or near-fixed value without moving those funds into the legitimate financial system into a fiat currency such as USD. Some examples of stablecoins include.

a. Tether (USDT) was developed by Tether Limited Inc. and is designed to maintain its value at $1.00 USD. USDT can utilize the existing ETH blockchain or the newer TRON ("TRX") blockchain.

b. Binance USD (BUSD), which was developed by Binance Holdings Limited and Paxos Trust Company, LLC, is designed to maintain its value at $1.00 USD. BUSD utilizes the existing ETH blockchain.

d. A digital currency exchange (an "exchange") is a business that allows customers to trade digital currencies for other digital or fiat currencies. An exchange can be a brick-and-mortar business, or strictly an online business. Both brick and mortar and online exchanges accept a wide variety of digital currencies, and exchange them for fiat and traditional payment methods, other digital currencies, or transfers between digital currency owners. Most exchanges are located outside the boundaries of the United States in order to avoid regulation and legal requirements, but some popular exchanges operate inside the jurisdiction of the United States. Binance is an example of a popular online exchange that is located outside of the United States but cooperates with and accepts legal process from American law enforcement agencies.

e. A wallet is a means of storing digital currency identified by unique electronic addresses that allows an individual to conduct transactions on the public ledger. To access a wallet on the public ledger, an individual must use a public address (or "public key") and a private address (or "private key"). The public address can be analogized to an account number while the private address is similar to a password used to access that account. Even though the public address of those engaging in digital currency transactions are recorded on the public ledger, the true

identities of the individuals or entities behind the public address are not recorded. If a real individual or entity is linked to a public address, however, it may be possible to determine what transactions were conducted by that individual or entity. Therefore, digital transactions are often described as "pseudonymous," meaning they are partially anonymous. Most individuals are identified when they use a digital currency exchanger to make a transaction between digital currency and fiat, or through digital currency exchangers that voluntarily or through legal order, cooperate with law enforcement.

f. What is common across many exploitations of the elderly and elder abuse cases when it comes to cryptocurrency, is that they initially contact the victim from a point of perceived authority to the victim. They do this through email, text message, and sometimes computer access through a point of compromise such as a virus or clicking a fraudulent link. This can be as sophisticated as impersonating law enforcement or purporting to be from their bank's corporate security. Once the suspect engages with the victims, they often request that they hide or lie about their actions as to not raise suspicion from actual authorities. From this point, they convince the victim to withdraw their own funds from their accounts and forward it to the suspect through various means. A common method it is to have the victim deposit cash into a Bitcoin ATM and send the transaction to a wallet address provided to the victim.

g. In 2023, K.W., a resident of Simpsonville, S.C. received a Telegram App call from a female who identified herself as Aggie Smith. She approached him about online investing in crypto currency. These calls evolved into video calls with this Aggie Smith, who convinced him to open and invest in a web platform called coinlink-web3, which is markedly similar to Chainlink-web3, which is a legitimate investment website. When K.W. made attempts to withdraw, he was prompted to pay fees in excess of $10,000.00. He attempted to make further communication with Aggie Smith, and make further efforts to withdraw the funds, but to no avail.

h. K.W. opened an account on the suspect trading platform and made numerous deposits into his account wallet addressed: 0x7F1392E44e1ef7578E486F0Ec33881cC3379AE3a. Over a several month period, K.W. made approximately 8 deposits into this wallet totaling around $135,000.00, believing this was a secure trading account that only he had access to. In reality, the funds were immediately moved out of his account into a wallet address that only served the purpose of receiving funds for a short period, compiling with other deposits and being forwarded on to other wallet addresses. This is often referred to as a Burn Wallet (Burn Wallet 1) . These wallets do not serve legitimate business purposes. The address of this Burn Wallet 1 is: 0x126cfc1Bb7e6424A2B25A98f8a1C27e2BF03EEc9. This wallet has been active for a little over four months and has received 58 transfers totaling approximately $1,176,296.00 USD. In each case, the funds are received, comingled with other

funds for a short period of time and then forwarded on to a handful of wallet addresses.

i. Special Agent ("SA") Joseph Lea ("Lea") reviewed transaction history for digital currency wallet 0x126cfc1Bb7e6424A2B25A98f8a1C27e2BF03EEc9 ("Burn Wallet 1") in a commercial blockchain analysis platform. Below is a summary of his review:

(1) On May 30, 2023, at 19:12Hrs 10,554 USDT was deposited into wallet 0x126cfc1Bb7e6424A2B25A98f8a1C27e2BF03EEc9 via transaction ID 0x8979364b9e2c8e5abd23037f7322ac31634341d6bcd5ccef7a02e45d347aaa48. Based on his training, experience and information from the victim, SA Lea believed this deposit was from K.W. and matched the account information provided to the Simpsonville Police Department. Those funds were quickly sent out to wallet 0xd106D00A1a5718a535995ac24C6551e12b714Ebc ("Burn Wallet 2").

j. SA Lea reviewed transaction history for digital currency wallet 0xd106D00A1a5718a535995ac24C6551e12b714Ebc (Burn Wallet 2) in a commercial blockchain analysis platform. This wallet was only active for two months, but during that time it received 81 transactions totaling $3,081,279.00. Below is a summary of his review:

(1) On May 30, 2023, ten minutes later at 19:22 Hrs 10,000 USDT was deposited into from 0x126cfc1Bb7e6424A2B25A98f8a1C27e2BF03EEc9 to wallet 0xd106D00A1a5718a535995ac24C6551e12b714Ebc (Burn Wallet 2) via transaction ID: 0xa4e00ebbfaca3f4f6838aedd751ee06bb622dd11e20d04c77cbf37a7892b9a65. Based on his training, experience and information from the victim, SA Lea believed this deposit was from the funds derived from victim K.W. From there the funds were quickly transferred to wallet 0xdb844629050C1921b8264Fb088bc4C3d16645432.

k. SA Lea reviewed transaction history for digital currency wallet 0xdb844629050C1921b8264Fb088bc4C3d16645432 (Suspect Wallet 1) in a commercial blockchain analysis platform. This wallet was active for a little over 8 months with regular activity, but during that time it received 782 transactions totaling $10,504,15.00. Below is a summary of his review:

(1) On June 2, 2023, at 04:20 Hrs., 10,000 USDT was deposited into from wallet 0xd106D00A1a5718a535995ac24C6551e12b714Ebc to wallet 0xdb844629050C1921b8264Fb088bc4C3d16645432(Suspect Wallet 1) via transaction ID: 0xd8887fc54d11552427e72904d89f1d7d919c64ac5716e4d0328622cda067605. Based on his training, experience and information from the victim, SA Lea believed this deposit was from the funds derived from victim K.W.

l. As discussed previously, Suspect Wallet 1 received numerous deposits from victims as a result of 18 U.S.C. §§ 1343 (Wire Fraud). As such, there is probable cause to believe that these transfers constituted the proceeds of the Subject Offenses.

m. On August 16, 2023, SA Lea reviewed transaction history in Suspect Wallet 1 provided by the hosting exchange, Binance:

(1) Binance identified GUO as the account holder of Suspect Wallet 1. The wallet became active in August 2021, but remained mostly inactive until January 2023. Since that time, Suspect Wallet 1 received 757 deposits totaling approximately $10,222,525.00, and sent 560 transactions totaling approximately $7,341,658.00. Of which, 549 withdrawals totaling $7,303,617.00 USDT go out to wallet TF9bkbuVnMjMCFiQ92JUbDgJfeBjxdWaWz ("Tron Burn Wallet 1"). Tron Burn Wallet 1 is a wallet address on the TRON network, which is known as a "Privacy Coin" and is often used by fraudsters in an attempt to obscure the source, nature, or ownership of the funds; and

(2) As it relates to tracing digital currency stolen from the victim discussed above, after the funds were deposited into the first suspect account Burn Wallet 1, the funds were divided between numerous wallet addresses. One particular other transfer is more distinctly described in a separate seizure affidavit. The other accounts can be described as wallets

held within the same fraud organization, all processing the transferring the fraudulently obtained funds in attempts to further obscure the nature, source, and ownership of the funds. Funds from Suspect Wallet 1 were even sent out over the TRON Network wallet TF9bkbuVnMjMCFiQ92JUbDgJfeBjxdWaWz which in turn transferred the funds to wallet address TJe7rkW5gUybkwDSm1DybHpVb7z9f625dh which is the TRON network address of the other suspect wallet as described earlier.

n. Based on SA Lea's training and experience, he believed Suspect Wallet 1 was used by the Subjects to receive proceeds from victims of wire fraud and to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds obtained from the scam. Therefore, there is probable cause that Suspect Wallet 1 was used to facilitate the commission of the Subject Offenses, contained proceeds of the Subject Offenses and is therefore subject to seizure and forfeiture.

o. The Subject Account bears numerous red flags for a money laundering facilitation account, namely:

(1) The volume of transactions in the Subject Account is highly suspicious, with more than $10 million in USD equivalent of digital currency moved through the wallet associated with the Subject Account in less than 8 months;

(2) The Subject Account does not appear to hold digital currency for long, instead rapidly receiving and then retransmitting digital currency, and often in the form of stablecoins;

(3) The Subject Account appears to immediately transfer the funds out through a privacy network called TRON;

(4) The Subject Account does not appear to be engaged in any investment activity, as digital currency is rapidly moved in and out, and stablecoins are designed not to increase in value greater than the USD;

(5) While these amounts might be unsurprising in a commercial or business account, the Subject Account was opened as a personal account with no identified associated business;

(6) Public information searches for GUO do not identify any legitimate businesses associated with GUO which would justify a personal account receiving and sending these volumes of digital currency; and

(7) The transaction activity in the Subject Account appears consistent with a "layering" account in a money laundering scheme, where an account is used primarily to receive and convert criminal proceeds before transmitting the proceed on to another recipient, thus disguising the source of the proceeds and frustrating asset recovery and law enforcement.

p. Based on SA Lea's own investigation, records provided by Binance, and SA Lea's own training and experience, he believed the Subject Account was used

by the Subjects primarily to receive proceeds of elderly abuse scams involving digital currency stolen from victims and to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds obtained from the scam. The Subject Account further concealed and disguised the nature of the proceeds by combining the numerous deposits and forwarding from the account via the TRON Network. Therefore, there is probable cause the Subject Account was used to facilitate the commission of the Subject Offenses, contains proceeds of the Subject Offenses of USDT (the Subject Funds) are subject to seizure and forfeiture.

8. Based on the information and allegations set forth herein, there is a factual basis to support a reasonable belief that the Government will be able to meet its burden of proof at trial to show that the Defendant Funds constitutes, or is traceable to:

a. property involved in wire fraud transactions or attempted wire fraud transactions in violation of 18 U.S.C. § 1343;

b. property involved in money laundering transactions or attempted transactions in violation of 18 U.S.C. §1956(a)(1)(A)(i), and/or § 1956(a)(1)(B)(i) and/or 1957;

c. property involved in an illegal money transmitting business, in violation of 18 U.S.C. § 1960;

d. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(c)(7);

e. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(h) and;

f. property involved in money transactions in criminally derived property, in violation of 18 U.S.C. § 1957.

CONCLUSION

10. By reason of these premises, and pursuant to 18 U.S.C. § 981(f) and 21 U.S.C. § 881(h), whereby the Plaintiff's right, title and interest in and to the Defendant Funds relates back to the commission of the act giving rise to the forfeiture, the Defendant Funds has become and is forfeited to the United States of America, to be disposed of pursuant to Supplemental Rule G(7)(c) for Admiralty or Maritime Claims and Asset Forfeiture Actions, 18 U.S.C. § 981(d), 21 U.S.C. § 881(e), and other applicable laws.

WHEREFORE, Plaintiff prays that due process issue to enforce the forfeiture of the Defendant Funds, *in rem*; that a Warrant for the Arrest of the Defendant Funds be issued; that due Notice be given to all interested persons to appear, make claim, answer and show cause why the forfeiture should not be decreed; that the Defendant Funds be decreed condemned and forfeited to the United States of America for disposition according to law; and that Plaintiff have such other and further relief as the Court may deem just and proper, together with the costs and disbursements of this action.

Respectfully submitted,

ADAIR F. BOROUGHS
UNITED STATES ATTORNEY

By: *s/Carrie Fisher Sherard*
Carrie Fisher Sherard #10134
Assistant United States Attorney
55 Beattie Place, Suite 700
Greenville, SC 29601
(864) 282-2100

October 17, 2023