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

UNITED STATES OF AMERICA, Plaintiff, v. 0.4157802 BITCOIN (BTC) and 90,922.262837 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 0.4157802 BITCOIN (BTC) and 90,922.262837 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 Defendants Funds consists of 0.4157802 BTC valued at approximately $10,883.67 in United States Currency and 90,922.262837 USDT valued at approximately $90,897.36 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 xxxxx2339 ("Subject Account") and under the name Ram Kumar ("KUMAR").

4. The USSS seized the 0.4157802 BTC & 90,922.262837 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 Defendants Funds have a total domestic value of approximately $101,781.03 in United States Currency.

KNOWN POTENTIAL CLAIMANTS

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

   a. Ram Kumar who may have an interest in the Defendants 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

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

fiat or conventional currencies) and is instead generated and controlled through computer software operating on a 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:

(1) 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.

(2) 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. On or about June 20, 2023, V.C., a 62 year-old resident of Easley, S.C. received a pop-up on her laptop computer, and she was essentially locked out. An unknown individual then began to converse with V.C. through remote access and instructed the victim that her computer was locked, and bank account had been compromised. V.C. was informed that a representative from their bank would be calling them to help secure her funds and unlock her laptop. Moments later, she received a call on her cellular phone from someone purporting to be from Wells Fargo, their financial institution. The person on the phone called from a number that caller ID indicated was Well Fargo. This individual instructed V.C. that her bank account at Wells Fargo had been compromised and that he would help her store it in a secure account while they investigated. He instructed her to travel to her bank and withdraw $14,000.00, and if the teller questioned her, to say that it was for home renovations as he warned that an employee at the bank may be involved in the account being compromised.

h. V.C. traveled to her bank and withdrew $14,000.00 in cash. She was then

instructed to go to the Gulf gas station at 1315 Crestview Rd, Easley, SC and go to a Bitcoin ATM machine. From there she deposited her cash and made two transactions totaling $14,000.00 and sent it to the cryptocurrency wallet address provided by the scammer. This wallet address is bc1qknmj9hqcvtkjxulk2shu4r6uvu8sxzved24722 ("Burn Wallet 1"). Once the victims sent the BTC to the wallet address provided, the suspect cut off all further communication. Special Agent ("SA") Joseph Lea ("Lea") reviewed transaction history for digital currency wallet bc1qknmj9hqcvtkjxulk2shu4r6uvu8sxzved24722 ("Burn Wallet 1") in a commercial blockchain analysis platform. Below is a summary of his review.

i. On June 20, 2023, at 23:40 hours (UDT) 0.115643 BTC was deposited into the wallet via transaction ID: 07dee0ec6c0d72533b155a796901575a868c0801deaf506768265109aaa10b25. Based on SA Lea's experience and information from the victim, he believed this deposit was from V.C. and matched the receipt the victim received from the BTC ATM and turned over to the Easley Police Department.

j. On June 20, 2023, at 23:40 hours (UDT) 0.269598 BTC was deposited into the wallet via transaction ID: e039221a2a2e24352f5723984ff4fec7d91e5ff4f6a3824931d06682351f1ae

8. Based on SA Lea's experience and information from the victim, he believed this deposit was from V.C. and matched the receipt the victim received from the BTC ATM and turned over to the Easley Police Department:

k. This wallet, Burn Wallet 1, first became active with these two deposits and only remained active for 6 days. The funds received from V.C. were transferred out to another wallet mere hours later. This occurred for the short life of the wallet totaling 17 deposits all of which appear to be from similar victim sources, and 4 withdrawals all to the same wallet address, 1DNcHne3vGKzAarr6xX3XsyYrixw4bv7W1, (Suspect Wallet 1), held with Binance under the name Kumar. This is common in these type of fraud schemes, where a wallet is created for the sole process of acting as an intermediary wallet or "burner wallet," between the victim's transaction and the destination account held by the scammer group. This creates another layer in an attempt to conceal the nature and ownership of the illicit funds:

l. Based on reports filed by several BTC ATM hosting companies, SA Lea learned the following: to date there have been numerous other purported victims of this same type of fraud and that have sent funds to various burner wallets that in turn send to the same Suspect Wallet 1.

m. As discussed previously, at various times over the past several months, 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.

n. On July 28th, 2023, SA Lea reviewed transaction history in Suspect Wallet 1 provided by the hosting exchange, Binance:

o. Binance identified Ram Kumar as the account holder of Suspect Wallet 1. Between November 14, 2022 and July 25, 2023, Suspect Wallet 1 received 85 deposits totaling approximately $1,448,629.78. These transactions came from approximately 16 different burner wallets. Of which, numerous have been reported by various financial institutions as wallets who have received funds through fraud, and more specifically, elderly exploitation fraud.

p. The funds received into Suspect Wallet 1, are immediately converted within minutes from BTC to USDT. These funds are then sent out to various wallets 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. Suspect Wallet 1 has converted funds and sent to wallets such as xxxxx4Lct, which has received approximately $43,000,000.00 in the last three months. This suggests the scope and sophistication of this purported fraud network.

q. 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.

r. On July 28, 2023, Binance placed a hold on Kumar's crypto account. Upon doing so, they provided SA Lea's information as a point of contact. That same day, an individual purporting to be Ram Kumar, and using the email address on file for Kumar contacted SA Lea. He inquired as to why there was a hold placed on the account. When asked as to the nature of the account. The individual stated, "I am a crypto trader. I do most of my work online in telegram groups. I trade btc for usdt for little margin…. They send me funds. I send them back usdt." With the "margin" and fees, this would make the transactions more in line with a money laundering operation, rather than typical business trading. Several rapid emails back and forth occurred, until it was requested that "Kumar" provide an up-to-date photo and ID to ensure SA Lea was speaking with the proper account holder. Upon doing so, the individual no longer contacted or replied to any emails. It is commonly known that these fraud groups have "mules" open the accounts, and then operational control of the accounts are controlled by the fraud group. This further confirms that this account was used by the fraud group to launder the funds received through illicit means

s. The Suspect Wallet 1 bears numerous red flags for a money laundering facilitation account, namely:

(1) The volume of transactions in the Suspect Wallet 1 is highly suspicious, with nearly $1.5 million in USD equivalent of digital currency moved through the wallet associated with the Suspect Wallet 1 in just a few months;

(2) The Suspect Wallet 1 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 Suspect Wallet 1 appears to immediately convert via OTC transactions at a loss of value, the original stolen types of digital currency into stablecoins before transferring the resulting digital currency via a privacy network called TRON;

(4) The conversions in the Suspect Wallet 1 appear to lack a business purpose, because the operator(s) of the Suspect Wallet 1 converted more than $1 million in BTC into USDT over numerous transactions, but these conversations have negative value once the sale is made and any transactions costs are considered;

(5) The Subject Wallet 1 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;

(6) While these amounts might be unsurprising in a commercial or business account, the Suspect Wallet 1 was opened as a personal account with no identified associated business;

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

(8) The transaction activity in the Suspect Wallet 1 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 his 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 selling BTC for USDT and then withdrawing the USDT 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 BTC and 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; 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, in violation of 18 U.S.C. § 1957.

CONCLUSION

9. 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 18, 2023