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

UNITED STATES OF AMERICA, Plaintiff, vs. 36,924.569515 TETHER CRYPTOCURRENCY (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 36,924.569515 Tether Crypto Currency ("USDT") valued at approximately $36,931.24 USD ("United States Dollars"), ("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 consist of 36,924.569515 Tether Crypto Currency USDT valued at approximately $36,931.24 U.S. dollars 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 xxxxx7807 (the "Suspect Wallet 1") and under the name of Hasibul Hasan ("HASAN").

4. The USSS seized the 36,924.569515 Tether Crypto Currency USDT valued at approximately $36,931.24 USD, 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 $36,931.24.00.

KNOWN POTENTIAL CLAIMANTS

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

   a. Hasibul Hasan 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 brief 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

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

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 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 actually 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. On or about August 30, 2023, J.P., a 68 year-old resident of Six Mile, S.C. received an email from Norton Anti-virus indicating that his purchase for $100.00 had been processed, and if he did not make the purchase, to call customer support at the number provided. He called the number and was disconnected, an unknown subject immediately called back and purported to be from Norton Anti-virus. They requested that he download AnyDesk (a remote computer access program) in order to process his refund. The unknown individual then began to converse with J.P. through this remote access, and instructed the victim that he would process his refund. Upon doing so, the unknown individual had the victim type in $100.00 for the refund amount. After doing so, the person on the call became irate and indicated that he typed in $10,000.00 and that Norton Antivirus would report him to the Sheriff's office and have him arrested if he did not return the funds. The victim checked his account and found that a credit for $10,000.00 had posted to his account. So J.P. agreed to return the funds. The caller instructed him to withdraw cash from his bank account and travel to a Bitcoin ATM to send the funds.

h. J.P. traveled to his bank and withdrew $10,000.00 in cash. He was then instructed to go to a Bitcoin ATM machine in Pendleton, SC to send the funds to an account provided to him by the suspect. The suspect provided a QR code that the victim used to send the currency to. That QR code translated to the

cryptocurrency wallet address, 18o6TfmgsEdKLGRGktkv4Jfh8B2koBUzUL (subject account). Once the victims sent the BTC to the wallet address provided, the suspect cut off all further communication. It was then that the victim checked his accounts further and realized that the credit deposited into his account came from his own savings account. It is believed that through the remote access in his computer and account access, the suspect made the transfer to further convince the victim to send the funds.

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

(1) On August 30, 2023, at 01:38 hours (UDT) 0.27113235 BTC was deposited into the wallet via transaction ID: 6144a149827fb807e72ba04cea77f13892d6e23e750341f6258c4d4dd617d830. Based on my experience and information from the victim, I believe this deposit was from J.P. and match the information provided by the victim and turned over to the Pickens County Sheriff's Office.

j. 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 this wallet has been blacklisted and identified as

one in which numerous victims have attempted to send funds to as part of a fraud scheme, but the account had already been blocked.

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

l. On September 12, 2023, SA Lea reviewed transaction history in Suspect Wallet 1 provided by the hosting exchange, Binance:

(1) Binance identified HASAN as the account holder of Suspect Wallet 1. The wallet became active in December 2022. Since that time, Suspect Wallet 1 received 32 deposits totaling approximately $66,228.31. Of which most incoming transactions were in BTC, which were then immediately converted to USDT at a cost of transaction fees. This account received numerous transactions from US based bitcoin ATM machines, these same companies blacklisted the suspect wallet address due to reports of fraud from the victims. These funds immediately being converted to USDT, further indicate that they were illicit and there is an overt attempt to conceal the nature, source, and ownership of the funds.

m. Based on SA Lea's training and experience, the agent concluded that 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.

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

(1) 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;

(2) 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;

(3) 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;

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

(5) 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.

o. Based on SA Lea's investigation, records provided by Binance, and Special Agent Lea's training and experience, the government believes Suspect Wallet 1 was used by Hasibul Hasan 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 Suspect Wallet 1 was used to facilitate the commission of the Subject Offenses, contains proceeds of the Subject Offenses of BTC and USDT (the Defendant 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

November 14, 2023