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

UNITED STATES OF AMERICA,	)	CIVIL ACTION NO.:
	)	
	)	
Plaintiff,	)	
	)	
vs.	)	
	)	
	)	
2,048.575822 USDT	)	
	)	
Defendant *in Rem*.	)	
	)	

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 2048.575822 ("USDT") valued at approximately $2,050.51 USD ("United States Dollars"), ("Defendant Funds"), pursuant to 18 U.S.C. § 981 (b), 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 constitute, or are traceable to:

a. property involved in wire fraud transactions or attempted wire fraud transactions in violation of 18 U.S.C. §§ 1343, 1349 and/or conspiracy to commit same;

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 2,048.575822 USDT valued at approximately $2,050.51 USD, obtained by agents with the United States Secret Service ("USSS") during an investigation into a transnational criminal organization running a romance scheme and social engineering scam. The funds were seized from a cryptocurrency custodial wallet under the control of Binance, identified by account number 527231086 (the "Subject Account) and xxxxx1ETMCV (the "Suspect Wallet 1") and under the name of Andrew Aya ("Aya").

4. The USSS seized the 2,048.575822 USDT valued at approximately $2,050.51 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 $2,050.51.

KNOWN POTENTIAL CLAIMANTS

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

a. Andrew Aya 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. United States Secret Service ("USSS") and local law enforcement agencies were investigating a transnational criminal organization running a romance scheme and social engineering scam. In brief summary, investigating agents determined that a fraud group has been using social engineering to contact vulnerable, often recently widowed individuals and develop a person relationship with the victim in a long ongoing effort to extort money from the victim. At the point the victim becomes aware of the scam, they have made numerous deposits via wire transmission and crypto transmission. By the time the victim becomes aware of the scam, most funds have been laundered and forwarded on past the point investigators can successfully locate the funds.

b. As set forth below, the Subject Account was used by the scammers to receive and launder proceeds of the above-described scheme. Where the Subject Funds cannot be directly traceable to the victims discussed in this affidavit, the Subject Funds are laundered or derivative property found in the same account as the digital currency stolen from victims of this scheme. The Subject Account was created and used primarily for the purpose of

laundering scheme proceeds, including outside of the United States. Therefore, there is probable cause to believe that the Subject Funds are subject to seizure and forfeiture by the United States.

c. 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 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.

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

d. 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 is 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:

i. 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.

ii. 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.

e. 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.

f. 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.

BACKGROUND ON ROMANCE SCAMS RELATING TO CRYPTOCURRENCY

8. What is common across many investment scams when it comes to cryptocurrency is that they initially contact the victim using social media. In these cases, the victim is often lured into a personal relationship over a long period of time in which funds are not discussed. When the suspect has the victim thoroughly committed, the request for some sort of financial assistance is initiated. Eventually the request becomes extensive and with the sense of urgency to prevent in depth questioning.

VICTIM S.C. LOSES DIGITAL CURRENCY IN THE SCAM

9. Based on conversations, emails and reports filed by S.C., S/A Lea learned the following,

a. Over the past year and a half, S.C., a resident of Greer, S.C. received communication from an individual who she eventually began a romantic relationship with. She was in regular communication with this individual to whom

she believed to be and individual working for a logging company in the Alaskan and Canadian Wilderness. Eventually, the suspect began to ask S.C for funds due to various emergency and unforeseen circumstances, as "he" needed money. Over the past year and a half, S.C. has sent hundreds of thousands of dollars via wire transmission and through crypto deposits. Of the wires sent, the accounts that received the funds also appear to belong to elderly females, who are likely similar victims and money mules for the suspects.

b. Later in the scheme, S.C. was instructed to send funds via crypto currency. S.C. was provided the cryptocurrency address xxxx0z75. S.C. sent funds to this address on numerous occasions and most recently on October 11, 2024.

10. Transaction history for digital currency wallet xxxx0z75 ("Burn Wallet 1") showed that on October 11, 2024, at 21:23 Hrs. 0.112081 BTC was deposited into the wallet via transaction ID: xxxx0z75 via transaction hash xxxx0e84. This deposit was from S.C. and matches the account information provided to the Greenville County Sheriff's Office. Those funds were quickly sent out to wallet xxxxTMCV ("Suspect Wallet") on October 11, 2024, at 21:40 Hrs. via transaction hash xxxxf440.

11. The Suspect Wallet became active in October 2022. Binance identified Aya as the account holder of the Suspect Wallet.

12. Transaction history for digital currency wallet xxxxTMCV (Suspect Wallet) revealed that this wallet was only active for two years. During that time, it received 188

transactions totaling $308, 556.12 and sent 486 transactions totaling approximately $273,007.84.

12. Immediately after the deposits occur in BTC, the funds are converted to USDT stable coin via the means of Binance Orders selling the funds. Approximately 17 minutes after receiving S.C.'s funds in BTC, the funds were converted to USDT.

13. The Suspect Wallet received numerous deposits from victims as a result of 18 U.S.C §§ 1343, 1349 (Wire Fraud, Conspiracy). These transfers constituted the proceeds of the fraud.

14. The Suspect Wallet was further used to receive fraud proceeds and conceal or disguise the nature, location, source, ownership and control of those proceeds.

15. The Subject Account tied to the Suspect Wallet is consistent with a money laundering account because:

a. The volume of transactions in the Subject Account is highly suspicious, with more than $500,000 in USD equivalent of digital currency moved through the wallet associated with the Subject Account in less than two years;

b. 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;

c. The Subject Account appears to immediately transfer the funds out through a privacy network called TRON;

d. 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;

e. 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;

f. Public information searches for Aya do not identify any legitimate businesses associated with Aya which would justify a personal account receiving and sending these volumes of digital currency; and

g. 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.

16. The Defendant 2,048.575822 USDT was seized from this Subject Account as traceable fraud proceeds and property involved in money laundering.

CONCLUSION

17. The Defendant Funds are subject to seizure pursuant to 18 U.S.C. § 981(b) and forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A) (rendering subject to forfeiture any property involved in a violation of 18 U.S.C. §§ 1956/1957) and § 981(a)(1)(C) (rendering subject

to forfeiture any property that constitutes or is derived from proceeds traceable to a violation of 18 U.S.C. §§ 1028, 1028A, 1343, 1344).

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,

BRYAN P. STIRLING
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
Carrie.A.Fisher@usdoj.gov

October 27, 2025