IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TENNESSEE
WESTERN DIVISION

United States of America, Plaintiff, v. Any and All Virtual Currency, Funds, Monies, and other things of value stored in or accessible at Binance associated with User ID 165978850, Defendant.	)	Civil No.

COMPLAINT FOR FORFEITURE *IN REM*

NOW COMES the United States of America, Plaintiff herein, by and through Kevin G. Ritz, United States Attorney for the Western District of Tennessee, in a civil cause of forfeiture, and respectfully states the following:

INTRODUCTION

1. This is a civil action in rem pursuant to 18 U.S.C. § 981(a)(1)(A) and (C). Procedures for this action are mandated by Rule G of the Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions and, to the extent applicable, 18 U.S.C. §§ 981, 983, and 984, and the Federal Rules of Civil Procedure.

2. This action seeks the forfeiture of all right, title, and interest in the above-captioned property because the property constitutes or is derived from proceeds of wire fraud and wire fraud conspiracy in violation of 18 U.S.C. §§ 1343 and 1349, and property involved in monetary transactions, money laundering, and conspiracy to commit same, in violation of 18 U.S.C. §§ 1956. As set forth more fully below, on or more conspirators identified herein, through fraud

misrepresented themselves as technical support and/or refund support and convinced a victim (identified herein as "Victim") based in Memphis, Tennessee to share her Memphis Credit Union bank account information with the suspects to receive a refund. The suspects instructed the victim, she received too large of a refund, which funds needed to be returned via Bitcoin to an account associated with phone number 573-825-8177, described more fully below and identified herein as the "SUBJECT ACCOUNT."

3. This Court has jurisdiction over this action commenced by the United States under 28 U.S.C. § 1345 and over this action for forfeiture under 28 U.S.C. § 1355(a). The Court has in rem jurisdiction over the defendant property under 28 U.S.C. § 1355(b).

4. This Court has venue pursuant to 28 U.S.C. §§ 1355 and 1395. Venue is proper because the acts or omissions giving rise to the forfeiture occurred in this district and the claim accrued in this district.

5. The defendant is all present and future interest in the following property: cryptocurrency, virtual currency, funds, monies, and other things of value (hereafter, "Cryptocurrency," "Ether," and "Tether") seized by the United States Secret Service (hereafter, "USSS") from a Binance Holdings Ltd d.b.a. "Binance" (which owns and operates the Binance cryptocurrency exchange) account associated with user ID 165978850 and email address sunsuc2204@outlook.com held in the name of Suneet Gautam, and all proceeds traceable thereto (the "SUBJECT ACCOUNT"). The Cryptocurrency was seized in the Western District of Tennessee pursuant to a federal Seizure Warrant for forfeiture that was executed by the USSS on Binance in and around March 31, 2023, and USSS received the funds on or about June 19, 2023.

6. Pursuant to Supplemental Rule G(2)(f), facts in support of a reasonable belief that the Government will be able to meet its burden of proof at trial are as follows and have been verified

by the attached Verification of United States Secret Service Special ("USSS") Agent Morgan Morgan.

THE WIRE FRAUD SCHEME AND MONETARY TRANSACTIONS

7. On or about February 28, 2023, the USSS Memphis field office was contacted by Sgt. D. Boggan, Memphis Police Department Economic Crimes Bureau, who requested the USSS Memphis office trace cryptocurrency involved in a local scam. Sgt. Boggan stated that M.G., while a resident in Memphis, Tennessee (Western District of Tennessee) clicked on a link in an email and a Microsoft Security window popped up stating that her computer was infected with a virus. The link M.G. clicked was believed to have been malware.

8. M.G. was instructed, through the pop-up window, to call technical support at 833-710-5095 due to inadequate security on her laptop. The Threat Actor (TA) told M.G. that she needed to update her security on her laptop and would need to pay Microsoft $154.90. M. G. agreed to the payment and gave her Bank of America credit card number to the TA on the other line. M. G.'s Bank of America statement showed a charge from Soft Connect Sales for $154.90 with a reference number/phone number of 8446997978.

9. On 02/21/2023, M. G. received a call from an individual purporting to represent Microsoft who stated there was a problem with her payment and she was overcharged. An additional investigation into 617-465-5067 revealed a VOIP number that comes back to Inteliquent, Inc. An email requesting additional information related to this number was sent to Inteliquent's legal department. The overcharged payment was to be refunded to M. G. via direct deposit into her bank account. The TA then stated that they "accidentally" deposited $15,000 instead of $150 and needed her to return that money in the form of Bitcoin. M. G. found this suspicious and questioned the caller. At this point the caller became aggressive and stated he would post all of M. G.'s personal

information on the dark web if she didn't comply with his request and return the money. M. G. did as instructed and withdrew $14,000 from her Memphis Credit Union bank account #2211 and subsequently deposited it into a Bitcoin ATM machine. She was instructed to transfer the funds to an account with phone number 573-825-8177. Investigation into this number revealed that it is an AT&T wireless number associated with an individual, L.S. out of Centralia, Missouri.

BACKGROUND OF CRYPTOCURRENCY

10. The following terms have the following meanings as set forth herein:

11. **Cryptocurrency and Blockchain Generally:** Cryptocurrency, a type of virtual currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are Bitcoin, Litecoin, and Ether. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud- based servers. Users of cryptocurrency use public and private keys to transfer cryptocurrency from one person or place to another. A public key is typically a set of numbers and/or letters that a cryptocurrency user shares with other users to engage in a transaction in cryptocurrency, whereas a private key is typically a set of numbers and/or letters that the user of an account maintains privately to access his or her cryptocurrency. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. As such, most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction. Although many cryptocurrencies are or purport to be pseudonymous, often law enforcement and currency exchangers can use the

blockchain to analyze transactions in cryptocurrency, identify individuals who are using cryptocurrency platforms for illicit purposes, and trace fraud proceeds from victims to one or more exchanges or wallets, discussed more fully below.

12. **Ether:** Ether ("ETH") is a psuedonymous cryptocurrency. In other words, although Ether transactions are visible on a public ledger, each transaction is referenced by a complex series of numbers and letters (as opposed to identifiable individuals) involved in the transaction. For this reason, although Ether has some legitimate uses, many criminal actors use Ether to defraud victims, engage in illicit transactions, and launder crime proceeds. Although Ether addresses are unique tokens, Ether is designed so that one person may easily operate many accounts, sending and receiving Ether through one Ether address or many different Ether addresses. For example, five addresses each holding five Ether can collectively send twenty-five Ether in a single transaction.

13. **Tether:** Tether, also known as "USDT," is a cryptocurrency generally recognized as a stablecoin—that is, Tether is designed to maintain the value of $1 USD per USDT coin.

14. **Wallets:** Cryptocurrency is often stored in a virtual account called a wallet, which can exist in, among other forms, an external computer device, a computer, on an application, or online. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. Access to a wallet and the cryptocurrency therein is typically protected by a password only known to the owner or user of the wallet.

15. **Exchangers, such as Binance and Coinbase:** Virtual currency "exchangers" and "exchanges" are individuals or companies that exchange virtual currency for other currencies, including U.S. dollars. Binance, which may be based in the Cayman Islands and/or elsewhere but also appears to maintain a subsidiary or affiliated company in the United States, and Coinbase are

full-service cryptocurrency exchangers and offer services to account holders. For example, Binance facilitates the purchase, sale, and transfer of a variety of digital currencies. Binance can identify accounts using a variety of target identifiers, including the identifiers provided herein for the SUBJECT ACCOUNT.

SUMMARY OF THE SCHEME INVOLVING SUBJECT ACCOUNT

16. The SUBJECT ACCOUNT consists of all virtual currency, funds, monies, and other things of value stored in or accessible at Binance associated with User ID 165978850, and email address sunsuc2204@outlook.com, held in the name of Suneet Gautam, and all proceeds traceable thereto.

17. The SUBJECT ACCOUNT is associated with the cryptocurrency wallet address: 13B9cBTZNMg1S5pFgRfreq4NSJX27uYTwP (hereinafter "wallet address ending in YTwP").

18. The SUBJECT ACCOUNT was opened online on or about May 21, 2021. The sole signatory on the SUBJECT ACCOUNT is Suneet Gautam, who opened the account using a Government of India Unique Identification Document.

19. Since the establishment of the SUBJECT ACCOUNT, multiple "Approved Devices" including iPhone XR, Suneet iPhone, Samsung SM-M307F, Mac Operating System device, Windows Operating System device has logged into the account. These devices logged in through multiple IP addresses which geolocates back to Dehli, India, Kashipur, India, and Noida, India.

20. Law enforcement agencies, including USSS Morgan Morgan, through training and experience have identified and linked Fraudulent Crypto App and Website scams to East Asian-based criminal enterprises that operate out of scam compounds predominately located in Cambodia, Laos, Thailand, and Myanmar.

21. Since account inception, there were 16 total deposits, totaling approximately $78,650.00 worth of cryptocurrency. These deposits were conducted on nearly a daily basis. Since account

inception, there were 14 total withdrawals, totaling approximately $62,100.00 worth of cryptocurrency. These withdrawals were conducted on nearly a daily basis.

22. On March 24, 2023, based upon a freeze request from this office, Binance froze the SUBJECT ACCOUNT, which contained the Bitcoin equivalent value of 0.69904803 BTC.

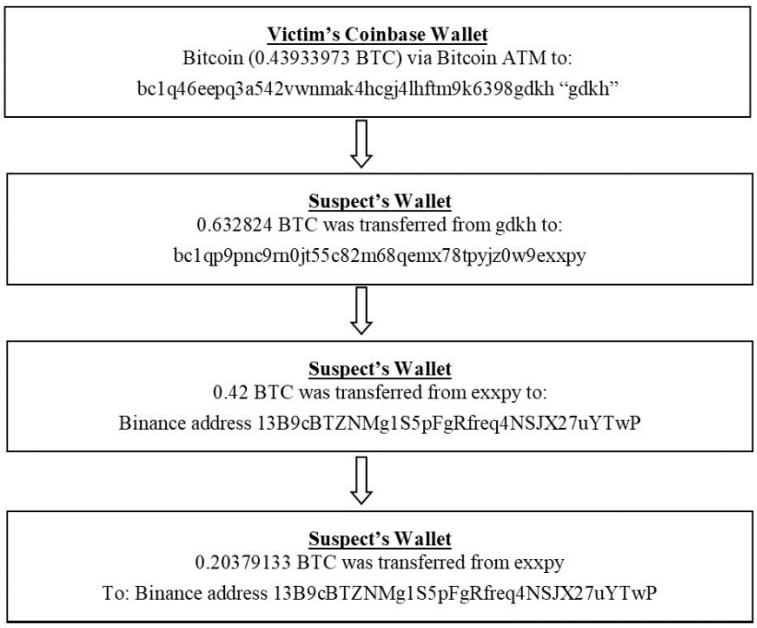
23. On or about February 21, 2023, M. G. transferred approximately $14,000.00 worth of Bitcoin (0.43933973 BTC) via Bitcoin ATM to: bc1q46eepq3a542vwnmak4hcgj4lhftm9k6398gdkh "gdkh".

24. Thereafter, on or about February 22, 2023, 0.632824 BTC was transferred from gdkh to bc1qp9pnc9rn0jt55c82m68qemx78tpyjz0w9exxpy.

25. Thereafter, on or about February 22, 2023, 0.42 BTC was transferred from exxpy to Binance address 13B9cBTZNMg1S5pFgRfreq4NSJX27uYTwP – SUBJECT ACCOUNT.

26. Thereafter, on or about February 25, 2023, 0.20379133 BTC was transferred from exxpy to Binance address 13B9cBTZNMg1S5pFgRfreq4NSJX27uYTwP – SUBJECT ACCOUNT.

The transactions are graphically summarized as follows:



CONCLUSION

27. Based on the foregoing, there is probable cause to believe that the SUBJECT ACCOUNT represents property traceable to proceeds of a wire fraud scheme, in violation of Title 18, United States Code, Sections 1343, and property involved in a money laundering scheme, in violation of Title 18, United States Code, Section 1956.

Respectfully submitted,

KEVIN G. RITZ
United States Attorney

By: s/ Reid Manning
REID MANNING
Assistant United States Attorney
800 Federal Bldg., 167 N. Main
Memphis, Tennessee 38103
(901) 544-4231

STATE OF TENNESSEE
COUNTY OF SHELBY

VERIFICATION

Morgan Morgan deposes and says under penalty or perjury:

I am a Special Agent with the United States Secret Service and one of the agents assigned to this case.

I have read the foregoing Complaint and the factual information contained therein is true according to the best of my knowledge, information, and belief.

s/ Morgan Morgan
Special Agent Morgan Morgan

September 15, 2023
Date