**IN THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF MISSOURI ST. JOSEPH DIVISION**

| | |
|---|---|
| UNITED STATES OF AMERICA,<br><br>Plaintiff,<br><br>v.<br><br>ASSORTMENT OF VIRTUAL CURRENCY ASSETS SEIZED FROM A BINANCE ACCOUNT,<br><br>Defendant. | Case No. |

## COMPLAINT FOR FORFEITURE IN REM

Plaintiff, United States of America, by its attorneys, Teresa A. Moore, United States Attorney for the Western District of Missouri, and John Constance, Assistant United States Attorney, brings this complaint and alleges as follows in accordance with Supplemental Rule G(2) of the Federal Rules of Civil Procedure:

## NATURE OF THE ACTION

1. This is an action to forfeit property to the United States pursuant to 18 U.S.C. § 981(a)(1)(C) based on violations of 18 U.S.C. §§ 1343 and 1956.

## THE DEFENDANT IN REM

2. The defendant property consists of approximately 43 virtual currency assets from Binance Account ID 26687339, an account held by Nest Services Limited, Mahé, Seychelles, that was seized on or about August 8, 2024 (the "Defendant

Property"). The Defendant Property is presently in the custody of the Federal Bureau of Investigation (FBI).

3. Binance completed the transfer of the contents of the defendant property to the FBI on or about November 19, 2024. The contents consist of the following approximate virtual currency amounts:

| Currency | Amount | Currency | Amount | Currency | Amount |
|---|---|---|---|---|---|
| AAVE | 141.699 | FUN | 122336 | SNX | 3272.892948 |
| ACH | 9293 | GRT | 3058 | SOL | 30.55 |
| ALGO | 5204.992 | HOT | 619238 | SUSHI | 3241.719 |
| APE | 244.28 | IOTA | 433.3782 | TRX | 4558.058117 |
| BLZ | 19408 | KAVA | 2556.57 | UMA | 97.61 |
| BNB | 1.03472011 | KNC | 66.67517152 | USDT | 1680.552724 |
| BTC | 4.8405018 | LINK | 204 | VIB | 44233 |
| COMP | 99.85 | LTC | 69.03803526 | VIC | 4929.6 |
| CREAM | 282.207 | MANA | 1031 | WIN | 3066438 |
| CRV | 1508.665 | MATIC | 4293.1 | WRX | 55,765.64 |
| DENT | 596419 | MDT | 897.8591 | XTZ | 701.9 |
| DOGE | 72753 | MKR | 0.98531 | YFI | 3.00463 |
| DOT | 500.35 | PUNDIX | 7062.587728 | ZRX | 3447.4 |
| ETC | 59.996 | SAND | 51 | | |
| ETH | 13.97773831 | SHIB | 587,268,885 | | |

## JURISDICTION AND VENUE

4. This Court has subject matter jurisdiction over an action commenced by the United States under 28 U.S.C. § 1345, and over an action for forfeiture under 28 U.S.C. § 1355(a). This Court also has jurisdiction over this particular action under 18 U.S.C. § 981(a).

5. This Court has *in rem* jurisdiction over the defendant property pursuant to 28 U.S.C. § 1355(b)(1)(A) because acts or omissions giving rise to the forfeiture

occurred in this district; and pursuant to 28 U.S.C. § 1355(b)(1)(B), incorporating 28 U.S.C. § 1395, because the Defendant Property was brought into this district following seizure outside of the United States.

6. Venue is proper in this district pursuant to 28 U.S.C. §1355(b)(1)(A) because acts or omissions giving rise to the forfeiture occurred in this district; and pursuant to 28 U.S.C. § 1395, because the Defendant Property was brought into this district following seizure outside of the United States.

## BASIS FOR FORFEITURE

7. The Defendant Property is subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 981(a)(1)(C), because it constitutes, is derived from, or is traceable to proceeds of "specified unlawful activity," as that term is defined in 18 U.S.C. § 1956(c)(7), or a conspiracy to commit "specified unlawful activity," and as property involved in money laundering, in violation of 18 U.S.C. § 1956.

## FACTUAL ALLEGATIONS

### I. Background on virtual currencies

8. Virtual currencies are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank like traditional fiat currencies such as the United States Dollar, but rather are generated and controlled through computer software. Bitcoin (BTC) and Ether (ETH) are currently two of the most popular virtual currencies. Although there are more than 15,000 cryptocurrencies in existence, the vast majority

of these currencies are inactive, discontinued, associated with fraudulent projects, or have negligible market capitalization.

9. Virtual currency addresses are the digital locations to which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of letters and numbers.

10. Many virtual currencies, including bitcoin, publicly record all their transactions on what is known as a blockchain. The blockchain is a distributed public transaction ledger containing an immutable and historical record of every transaction utilizing that blockchain's technology.

11. Although generally the owners of virtual currency addresses are not known unless the information is made public by the owner (for example, by posting the address in an online forum or providing the address to another user for a transaction), analyzing the blockchain can sometimes lead to identifying both the owner of an address and any other accounts that the person or entity owns and controls.

12. Virtual currencies often are transacted using an exchange, which is a virtual currency trading and storage platform. An exchange typically allows trading between the U.S. dollar, foreign currencies, bitcoin, and other virtual currencies. Many virtual currency exchanges also store their customers' virtual currencies in digital wallets. These exchanges act as money services businesses. Binance operates the largest virtual currency trading platform in the world.

13. Because most virtual currency blockchains are public and can be traced by law enforcement using blockchain analytics tools, criminal actors attempt to disguise the origins and destinations of illicit virtual currency funds through a variety of means. Common virtual currency money laundering behaviors include rapidly moving funds between different virtual currency addresses without apparent business rationale, converting across different virtual currency blockchains (i.e., "chain-hopping"), transferring bitcoin in large volumes in exchange for currencies held on a decentralized blockchain platform (e.g., TRON), receiving a large volume of low value virtual currency deposits from numerous addresses and aggregating funds into large volume transfers to select number of different addresses (e.g. a "mule" or "funnel" account), and transferring funds from countries commonly targeted by cyber fraud, such at the United States, to jurisdictions known for weak regulatory frameworks, inadequate anti-money laundering controls, or heightened levels of corruption.

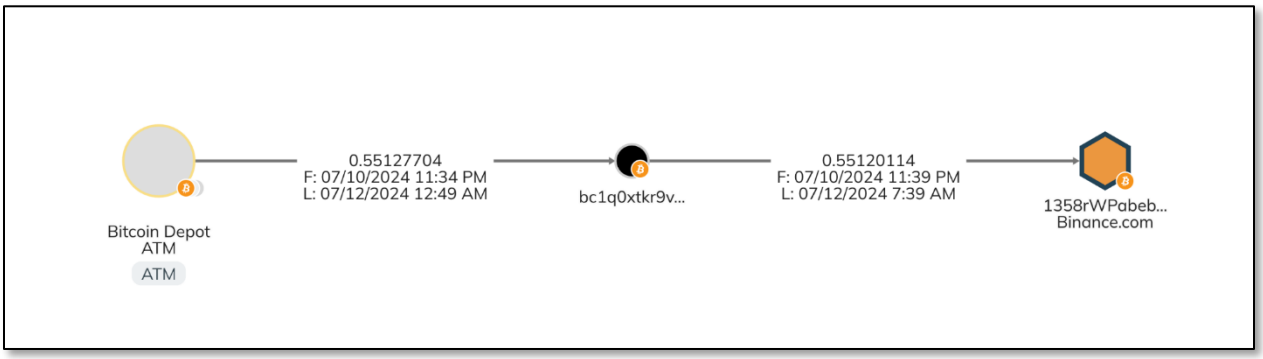
## II. Links between Subject Account and virtual currency confidence scam

*i. Victim 1*

14. On July 10, 2024, "Victim 1," who resides in Platte County, Missouri, received a text message that appeared to be from Victim 1's insurance company. Victim 1 clicked on the hyperlink embedded in the message and began an online conversation with an individual named "Richard" who claimed to be an insurance agent. Richard asked Victim 1 to pay Victim 1's insurance coverage using

cryptocurrency. Victim 1 withdrew cash from the bank and took the money to a bitcoin-based automated teller machine ("BTM") operated by Bitcoin Depot. Bitcoin Depot operates BTMs that convert fiat currency (general government currency like dollars, Euros, or pounds) into cryptocurrency. Victim 1 transferred Bitcoin to the individual he believed to be Richard to pay for his insurance premium.

15. Between July 10 and July 12, 2024, Victim 1 sent approximately 0.5512 Bitcoin (equaling approximately $45,000, including transaction fees) to a cryptocurrency wallet address provided to him by Richard. An unknown party then moved the funds from "Richard's" wallet to Binance account 26687339—the "Subject Account"—within mere minutes to hours of Victim 1's deposits. The diagram below depicts the movement of Bitcoin from Victim 1 to the Subject Account.




16. The Subject Account was registered to Nikhil Agarwal, who is believed to be an Indian citizen residing in Kolkata, India.

17. After Victim 1's 0.5515 Bitcoin were deposited into the Subject Account, they were exchanged for approximately 31,791.47 Tether, another virtual currency.[1] On July 15, 2024, 39,000 Tether was transferred from the Subject Account to a wallet address ending in -AZR3jfq associated with the TRON Network, a decentralized, blockchain-based operating system.

18. TRON's low transaction fees, anonymity, and quick transaction speeds are attractive to transnational criminal actors seeking to obfuscate the origins and destinations of illicitly obtained funds.

*ii. Victim 2*

19. On February 16, 2022, the Subject Account received approximately .3279 Bitcoin and 10.2492 Ethereum from a Coinbase account belonging to an elderly individual in Studio City, California ("Victim 2").

20. Victim 2 received an email that he believed to have been sent from Paypal saying there was a problem with his account and directing him to number to call for support.

21. Victim 2 called the number and was connected with a man speaking in an Indian accent. He was directed by the man on the phone to grant remote access to his computer, which Victim 2 did. Victim 2 was instructed that the Paypal problem

[1] "Tether" (which is traded under the "USDT" symbol) is a blockchain-based cryptocurrency whose tokens in circulation are backed by an equivalent amount of U.S. dollars, making it a stablecoin with a price pegged to USD $1.00.

would be resolved after 30 minutes and to remain off of his computer during that time.

22. After Victim 2 reconnected, he noticed that approximately $152,000 worth of virtual currency was had been transferred from his Coinbase account.

*iii. Victim 3*

23. In or around March 2022, an individual in California, ("Victim 3") received an email purporting to be from Paypal saying there was something wrong with Victim 3's account and directing Victim 3 to call a support number.

24. Victim 3 called the number and spoke to someone with a non-American accent. To regain access, Victim 3 was directed to send $13,500 via wire transfer to a JP Morgan Bank account. The funds were transferred soon after to a Gemini account belonging to an elderly man in Fontana, California.

25. Between March 15, 2022, and June 14, 2022, the Subject Account received approximately 1.6529 Bitcoin from the Gemini account. The only activity in the Gemini account is incoming wire transfers—like those from Victim 3—which were used to purchase Bitcoin. The Bitcoin was transferred to the Gemini account on the same day of purchase and then moved to the Subject Account.

*iv. The Subject Account received funds from multiple additional unidentified victims*

26. A blockchain analysis of Subject Account activity reveals multiple additional transfers between 2021 and 2023 consistent with the receipt and transfer of funds obtained from victims through fraud.

27. On May 6, 2023, the Subject Account received approximately 0.1947 Bitcoin from a Bitcoin Depot account. As with Victim 1's funds, these funds were nearly immediately thereafter exchanged the Bitcoin for approximately 5,741.79 Tether, and subsequently transferred the Tether funds from the Subject Account to the TRON-associated address ending in -AZR3jfq.

28. On May 9, 2023, the Subject Account received approximately 0.2724 Bitcoin from a CoinHub BTM account. Minutes later, the Bitcoin was exchanged for approximately 7,537.53 Tether. On May 10, 2023, two transfers were made from the Subject Account to separate wallet addresses associated with the TRON network.

29. On June 29, 2023, the Subject Account received approximately 0.2734 Bitcoin from a Bitcoin Depot BTM. The Bitcoin was exchanged for approximately 8,221.96 Tether and then transferred the Tether from the Subject Account to the TRON-associated address ending in -AZR3jfq.

30. Upon information and belief, Bitcoin Depot BTMs are located only in the United States of America and Canada and Coinhub BTMs are located only in the United States. As noted above, Agarwal is believed to be residing in India.

31. Between June 28, 2021, and February 9, 2023, the Subject Account received 17 transfers from four different Paxful accounts (another cryptocurrency exchange) totaling 3.7924 Bitcoin. One account, Nikhil199724, was in the name of Nikhil Agarwal. The second and third accounts, Tradingislove and Tradingislife, belong to two other individuals using Indian documentation. The fourth account, IntegritySoul05, was in the name of an individual using a Kenyan identification.

32. All four Paxful accounts were funded primarily by gift cards and payments from money transfer services, such as Cash App and Paypal. The Nikhil199727 account purchased approximately $1.6 million in virtual currency using 45 different gift cards and money transfer services.

33. Gifts cards are commonly used to launder illicit proceeds from fraud victims because the funds can be easily, quickly, and anonymously transferred anywhere in the world.

## CLAIMS FOR RELIEF

### FIRST CLAIM FOR RELIEF

34. The Plaintiff repeats and incorporates by reference the paragraphs above.

35. By the foregoing and other acts, the Defendant Property, constitutes, or was derived from, proceeds traceable to specified unlawful activity, and therefore, is forfeitable to the United States, pursuant to 18 U.S.C. § 981(a)(1)(C).

### SECOND CLAIM FOR RELIEF

36. The Plaintiff repeats and incorporates by reference paragraphs 1–31 above.

37. By the foregoing and other acts, the Defendant Property constitutes property involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956, or is traceable to such property, and therefore, is forfeitable to the United States, pursuant to 18 U.S.C. § 981(a)(1)(A).

WHEREFORE the United States prays that the Defendant Property be forfeited to the United States, that the plaintiff be awarded its costs and disbursements in this action, and for such other and further relief as the Court deems proper and just.

Respectfully submitted,

Teresa A. Moore
United States Attorney

By: */s/ John Constance*

John Constance
Assistant United States Attorney
400 E. 9th Street, Fifth Floor
Kansas City, Missouri 64106
Telephone: (816) 426-3122
E-mail: John.Constance@usdoj.gov

## VERIFICATION

I, Special Agent Melanie Wascom, hereby verify and declare under penalty of perjury that I am a Special Agent with the Federal Bureau of Investigation, that I have read the foregoing Verified Complaint *in Rem* and know the contents thereof, and that the factual matters contained in paragraphs 8 through 33 of the Verified Complaint are true to my own knowledge, except that those matters herein stated to be alleged on information and belief and as to those matters I believe them to be true.

The sources of my knowledge and information and the grounds of my belief are the official files and records of the United States, information supplied to me by other law enforcement officers, as well as my investigation of this case, together with others, as a Special Agent of the Federal Bureau of Investigation.

I hereby verify and declare under penalty of perjury that the foregoing is true and correct.

Dated 12/31/2024

*/s/ Melanie Wascom*
Melanie Wascom
Special Agent
Federal Bureau of Investigation