UNITED STATES DISTRICT COURT
DISTRICT OF CONNECTICUT

UNITED STATES OF AMERICA, *Plaintiff*, v. THE CONTENTS OF BITCOIN WALLET ENDING IN "pS4Z", HELD IN THE NAME OF ALOK KUMAR SINGH, AT BINANCE, *Defendant*,	No. 3:24 MC 24 (SDV)

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEIZURE WARRANT

I, Geoffrey Goodwin, being duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I am a Special Agent with Immigration and Customs Enforcement, Homeland Security Investigations ("HSI"). I have been a Special Agent with HSI since February 2006 and am currently assigned to the Hartford, CT Office of Investigations. As a Special Agent with HSI, I have conducted and participated in investigations involving identity theft, access device fraud, wire fraud, mail fraud, bank fraud and other financial crimes. I have further obtained and executed search, arrest, and seizure warrants. As an HSI Special Agent, I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code. That is, I am an officer of the United States, who is empowered by law to conduct investigations of and make arrests for offenses enumerated in Title 18 of the United States Code.

2. I make this affidavit pursuant to 18 U.S.C. § 1343, Wire Fraud, and 18 U.S.C. § 1956, Money Laundering, in support of an application for a seizure warrant for the contents of Bitcoin wallet "1KKLz5GFLkJcNkVh7rBvXhTxCNwQ3FpS4Z", held in the name of Alok Kumar SINGH, at Binance ("TARGET WALLET"), as a direct result of deposits made by

victims R.M. and A.D. and traced into the target wallet between January 30, 2024, and February 2, 2024 and because this account is "involved in" money laundering.

3. I believe that that probable cause exists to believe that the contents of the TARGET WALLET were obtained knowingly by a scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice in violation of 18 U.S.C. § 1343, and that these funds are subject to forfeiture pursuant to civil forfeiture under 18 U.S.C. § 981(a)(1)(C) for the forfeiture of property which constitutes or is derived from proceeds traceable to an offense constituting "specified unlawful activity" (as defined in 18 U.S.C. §§ 1956(c)(7) and 1961(1)), namely wire fraud in violation of 18 U.S.C. § 1343, or conspiracy to commit such offense, and criminal forfeiture under 18 U.S.C. 981(a)(1)(A) via 18 U.S.C. § 1956(c)(7)(A) (defining specified unlawful activities to include offenses listed in 18 U.S.C. § 1961(1)), 18 U.S.C. § 1961(1) (covering 18 U.S.C. § 1343), and 28 U.S.C. § 2461 (permitting criminal forfeiture if civil forfeiture is permitted) for violations of 18 U.S.C. § 1343. Additionally, I believe that the TARGET WALLET is involved in Money Laundering in violation of 18 U.S.C. § 1956 and is subject to civil forfeiture under 18 U.S.C. § 981(a)(1)(A) and criminal forfeiture under 18 U.S.C. § 982(a)(1).

4. I request that the Court issue a seizure warrant for the TARGET WALLET pursuant to 18 U.S.C. § 981(b), 18 U.S.C. § 982(b)(1), and 21 U.S.C. § 853(f).

5. The facts in this Affidavit come from my personal observations, my training and experience, witness information, and information obtained from other law enforcement officers.

This Affidavit is intended to show merely that there is sufficient probable cause for the issuance of the requested seizure warrant and does not set forth all the information law enforcement officers have learned in this investigation.

BACKGROUND OF INVESTIGATION

7. Your Affiant is currently investigating a fraud scheme in which at least one unknown individual took various steps to defraud at least two known victims in this case, including directing them to send Bitcoin through Bitcoin ATM kiosks to a suspect controlled wallet.

8. A fraud scheme such as this involves the victim receiving a call/e-mail/text message stating one of their financial accounts is compromised. The message directs the victim to contact "customer support" immediately. Upon contacting the number provided for "customer support," the suspects gain access to the victim's computers via remote desktop software and makes it appear the victim was accidentally "overpaid" and needs to refund the money immediately. The victims are instructed to withdraw that "overpayment" and are then directed to local Bitcoin ATM's for deposit. Victims are told not to contact law enforcement or to hang up the phone.

9. Upon arrival at those Bitcoin ATM's, victims are told to deposit funds into those Bitcoin ATMs and deposit those funds into specific Bitcoin wallets which the fraudsters typically have control over. Often, the fraudsters will then rapidly move those funds out of the initial Bitcoin wallets funds were deposited into, and disburse those funds into additional cryptocurrency wallets, potentially multiple times. Ultimately, the fraudsters may attempt to conduct cash withdrawals from those cryptocurrency wallets as a final step of "liquidation," or as a step taken to make additional tracing substantially more difficult for law enforcement.

CRYPTOCURRENCY, TRACING AND ASSOCIATED TERMINOLOGY

10. 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.

11. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys used to transfer cryptocurrency from one person to another can be printed or written on a piece of paper or other tangible object. 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.

12. 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. Cryptocurrency is not illegal in the United States and the vast majority of cryptocurrency transactions are for legitimate and legal purposes. There are, however, many ways in which criminals exploit cryptocurrency for illicit activity.

13. Bitcoin (BTC) is a type of cryptocurrency. Payments or transfers of value made with bitcoin are recorded on the blockchain network. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public

address or key. To conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key"). A public address is represented as a case-sensitive string of letters and numbers, 26 to 36 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key - the cryptographic equivalent of a password or PIN - needed to access the address.

14. Cryptocurrency "exchangers" and "exchanges" are individuals or companies that exchange bitcoin for other currencies and cryptocurrencies, including U.S. dollars. According to the Department of Treasury, Financial Crimes Enforcement Network ("FinCEN") Guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses. They are subject to certain regulatory requirements, such as collecting know-your-customer (KYC) information for its users.

15. As noted above, all cryptocurrency transactions are recorded on the blockchain, which becomes a public ledger. The transaction data available on the blockchain allows investigators to trace the flow of funds from one address to another. The limitation of the publicly available blockchain is that the addresses are not associated with any real-world entities. To address this problem, law enforcement will utilize proprietary blockchain analysis tools to create a visual representation of the flow of funds and attribute certain addresses to real world entities, such as cryptocurrency exchanges. If funds are ultimately identified as being held on an account at a cryptocurrency exchange, such as Binance, legal process can be served on that exchange to affect a seizure of the illicit proceeds much akin to how US dollars can be seized from a bank account. The Westport Police Department (WPD) utilized software from TRM to trace the flow of funds in the case. TRM is a company which, according to their website,

"provides blockchain data with advanced analytics to help financial institutions and governments fight fraud, money laundering, and financial crime."

FACTS IN SUPPORT OF PROBABLE CAUSE

16. On February 1, 2024, R.M. came to Westport Police Department (WPD) Headquarters (HQ), and spoke with WPD Detective (DET) James Baker, to report that R.M. had been the victim of a Bitcoin ATM scam. Upon arrival at Westport PD, R.M. stated that he had received a phone call from a now suspected fraudster utilizing phone number 470-401-6509. R.M. stated that the fraudster claimed to be an employee of "PayPal" and advised R.M. that there was a fraudulent purchase on R.M.'s account. The fraudster then attempted to assist R.M. with "securing his accounts" in a claimed effort to prevent additional losses to R.M.

17. According to R.M., during this process the fraudster gained access to both R.M.'s computer and bank account. Furthermore, it appears the fraudster conducted an overpayment scam in which the fraudster made it appear to R.M. that too much money had been paid into R.M.'s account. The fraudster then urged R.M. to withdraw the money from his local bank and subsequently send it to the fraudster via a Bitcoin ATM.

18. R.M. stated that later on the same date, R.M. withdrew $15,300.00 United States Dollars (USD) from R.M.'s Chase bank account ending in 1985. The fraudster then first directed R.M. to a Bitcoin ATM located at 210 Danbury Rd. Wilton, CT 06897.

19. Upon arrival R.M. deposited $2,500.00 USD into that ATM, which converted to approximately .04511100 in Bitcoin, and those funds were then sent to Bitcoin wallet "bc1q8s83e6d8dxd36u5rylg7ma8c0r8ddc4drkn42w". R.M. stated that the Bitcoin ATM appeared to have a $2,500.00 USD limit of deposit on the machine, which R.M. relayed to the fraudster. The fraudster then directed R.M. to a Cash2Bitcoin ATM located 219 East Avenue

Norwalk, CT 06855.

20. R.M. stated that R.M. then deposited $12,800.00 USD into the Cash2Bitcoin ATM located at 219 East Avenue, Norwalk, CT and attempted to send it to Bitcoin Wallet "bc1q8s83e6d8dxd36u5rylg7ma8c0r8ddc4drkn42w".

21. R.M. stated that, during this process, Cash2Bitcoin ATM compliance contacted R.M. and explained that, due to Cash2Bitcoin's observations, R.M. was likely participating in a fraud scam. R.M. stated that he then hung up with the fraudsters. This resulted in R.M. not completing the transfer of $12,800.00 USD into Bitcoin Wallet "bc1q8s83e6d8dxd36u5rylg7ma8c0r8ddc4drkn42w".

22. Subsequently, WPD DET Baker conducted a trace of the $2,500.00 USD converted to Bitcoin that was sent from the Bitcoin Depot ATM. At the time of R.M.'s report, the funds deposited by R.M. appeared to remain in the original Bitcoin wallet. As a result, WPD DET Baker placed an alert for any incoming and outgoing activity on the wallet.

23. During the interview with R.M., WPD DET Baker observed that .04504 Bitcoin, or approximately $1,909.00 USD, had left Bitcoin wallet "bc1q8s83e6d8dxd36u5rylg7ma8c0r8ddc4drkn42w" and was sent to Bitcoin wallet "bc1q0n8s7hwp4z4qzjv4m0yhljz5x5576aqfc9lend". Based on previous transaction history, Bitcoin wallet "bc1q0n8s7hwp4z4qzjv4m0yhljz5x5576aqfc9lend" had only withdrawn money via crypto exchange "Binance" via Bitcoin wallet "16Wjd1czG9ttvaRSgsAGfoHZMaMwW4JJnp".

24. WPD DET Baker submitted a request for information to Binance connected to Bitcoin wallet "16Wjd1czG9ttvaRSgsAGfoHZMaMwW4JJnp". WPD DET Baker also contacted investigators from Binance and requested that

"bc1q0n8s7hwp4z4qzjv4m0yhljz5x5576aqfc9lend" be "blacklisted" to ensure that any funds from this wallet that are sent to Binance will be frozen, to which Binance complied.

25. On February 4, 2024, WPD DET Baker received an alert indicating funds had left Bitcoin Wallet "bc1q0n8s7hwp4z4qzjv4m0yhljz5x5576aqfc9lend". Information showed that approximately .616 Bitcoin was sent to Bitcoin wallet "1KKLz5GFLkJcNkVh7rBvXhTxCNwQ3FpS4Z", the TARGET WALLET. WPD DET Baker confirmed with Binance that these funds were currently frozen. WPD DET Baker then submitted a formal freeze funds request to Binance regarding Bitcoin wallet "1KKLz5GFLkJcNkVh7rBvXhTxCNwQ3FpS4Z", the TARGET WALLET, to which Binance again complied.

26. Binance then provided information showing that TARGET WALLET was associated with User ID 422706648, email address "as5424978@gmail.com", and the name Alok Kumar SINGH. An Income Tax Department Identification from the country of India appearing to belong to SINGH was also associated with the account.

27. WPD DET Baker then attempted to contact SINGH at the telephone number attached to the profile for the TARGET WALLET. WPD DET Baker spoke to an individual identifying themselves as SINGH, and hereafter referred to as SINGH, and SINGH stated that he receives Bitcoin as part of a job he found on Telegram. SINGH stated that he then exchanges the Bitcoin to "Tether" tokens, a different cryptocurrency, and SINGH earns a commission for each transaction. WPD DET Baker informed SINGH that the funds had been frozen within SINGH's Bitcoin wallet "1KKLz5GFLkJcNkVh7rBvXhTxCNwQ3FpS4Z", the TARGET WALLET, and that a search and seizure warrant would be applied for in connection with those funds.

28. WPD DET Baker observed the TARGET WALLET has been associated with

SINGH since March 14, 2022. The TARGET WALLET has conducted 45 inbound transactions totaling 10.140985 BTC valued at $360,866 and 37 outbound transactions totaling 10.140985 BTC valued at $360,175. WPD DET Baker observed the pattern that 1 or more inbound transactions would be pooled and usually sent to Binance on the same day. Using TRM tracing, WPD DET Baker observed approximately $314,200 (87%) of the incoming transactions can be traced to Cash-to-Crypto ATM services.

29. WPD DET Baker then conducted a reverse trace for the comingled funds in the TARGET WALLET. WPD DET Baker observed 3 initial transactions on January 30, 2024, that were attributed to Bitcoin ATM Kiosks. The first transaction appeared on January 30, 2024, at approximately 2:42 PM EST. Based on TRM tracing software, this transaction bore transaction hash "a496220e7a6780321877237adfcd51eeb04d616b35a3a7e1b1c2269ac5b835d1" and was conducted a Bitcoin Depot ATM for approximately .176898 Bitcoin. Those funds were sent to Bitcoin wallet "bc1qjx3y35srltp2vualqqdrvn2htjslrcta6fqudt".

30. The next transaction appeared to have occurred on January 30, 2024, at 3:46 PM EST. Based on TRM tracing software, this transaction bore transaction hash "61e56f33a35fd7f16daa3ead4c32dc9a11a21dc710926decbdd5bca7689fade2" and was conducted at a Bitcoin Depot ATM for approximately .08813. Those funds were then sent to Bitcoin wallet "bc1qjx3y35srltp2vualqqdrvn2htjslrcta6fqudt".

31. The next transaction also appeared to have occurred on January 30, 2024, at 6:48 PM EST. Based on TRM tracing software, this transaction bore transaction hash "5b593d1d64a64397b71b1c7e9595c396b3bb7d382a072acfac2087e250ce9410" and was conducted at a RockltCoin ATM for approximately .07870192 Bitcoin. Those funds were sent to Bitcoin wallet "bc1qjx3y35srltp2vualqqdrvn2htjslrcta6fqudt".

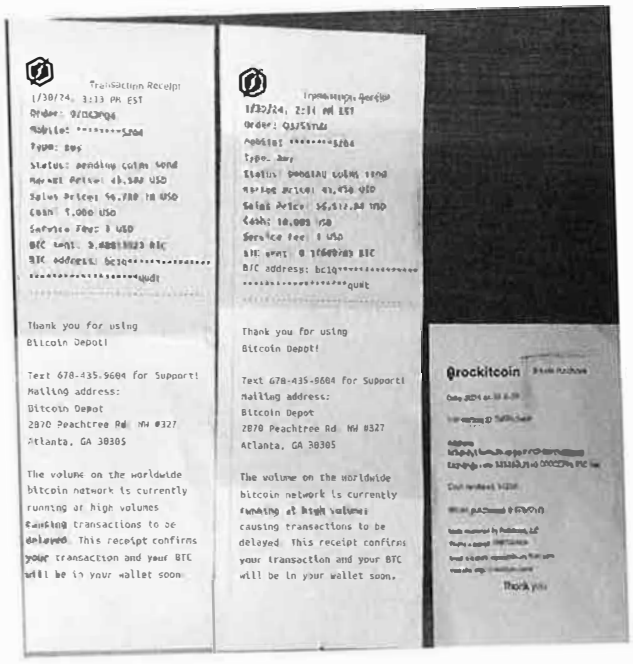
32. Subsequently, these funds appeared to be gathered together in Bitcoin wallet "bc1qjx3y35srltp2vualqqdrvn2htjslrcta6fqudt", along with two additional unidentified deposits. The entire balance of the Bitcoin wallet, approximately .55164445 Bitcoin, was then sent to Bitcoin wallet "bc1q0n8s7hwp4z4qzjv4m0yhljz5x5576aqfc9lend" on February 1, 2024 at 10:30 AM EST. Those funds were then co-mingled with R.M.'s fraudulently stolen Bitcoin.

33. On February 2, 2024, at 12:58 PM EST, approximately .616 Bitcoin was sent to the TARGET WALLET. Upon arrival, the .616 Bitcoin was frozen immediately as stated above.

34. On February 6, 2024, HSI Criminal Analyst (CA) Josh Cameron submitted Summons requests to Bitcoin Depot and RockItCoin for the above listed transactions.

35. On February 12, 2024, HSI CA Cameron provided WPD DET Baker with the RockItCoin Summons return. Information from that return showed that RockItCoin identified a possible victim as A.D. from Waynesboro, PA. On February 12, 2024, WPD DET Baker spoke with A.D. telephonically and informed her of the investigation.

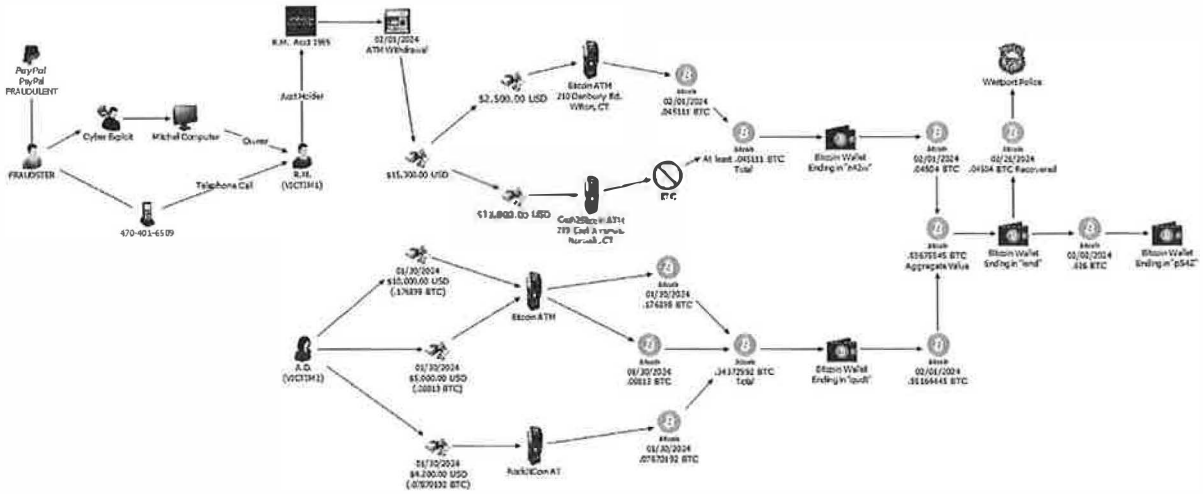
36. During that conversation, A.D. stated that she was the victim of a similar scam as R.M., and A.D. stated that she had made 3 separate Bitcoin transactions on 01/30/2024. A.D. provided pictures via email of the three Bitcoin ATM receipts. A.D.'s receipts matched the transactions listed above for Bitcoin Depot and RockItCoin. Furthermore, they show the January 30, 2024 transactions at $10,000.00 USD for .176898 Bitcoin, $5,000.00 USD for .08813 Bitcoin, and $4,200.00 USD for .07870192 Bitcoin. A.D.'s total loss of Bitcoin was .34372992 Bitcoin.



37. As of February 26, 2023, WPD DET Baker had successfully seized .04504 BTC from Bitcoin Wallet "bc1q0n8s7hwp4z4qzjv4m0yhljz5x5576aqfc9lend" via State of CT Seizure Warrant.

38. On February 13, 2024, and again on February 26, 2024, WPD DET Baker spoke with your Affiant regarding this investigation and provided your Affiant with the relevant information contained within this Affidavit.

39. The following is a visual depiction of the facts and circumstances articulated in the above paragraphs:



40. At the time of this Affidavit, it appears that .616 Bitcoin is contained within the TARGET WALLET.

LEFT BLANK INTENTIONALLY

CONCLUSION

41. Based on the foregoing information set forth above, I submit that probable cause exists to believe that the contents of the TARGET WALLET were obtained from wire fraud in violation of 18 U.S.C. § 1343, and that the TARGET WALLET is involved in money laundering in violation of 18 U.S.C. § 1956, and I request that the Court issue a seizure warrant pursuant to pursuant to 18 U.S.C. § 981(b), 18 U.S.C. § 982(b)(1), and 21 U.S.C. § 853(f).

GEOFFREY M GOODWIN Digitally signed by GEOFFREY M GOODWIN Date: 2024.03.01 08:30:36 -05'00'

GEOFFREY GOODWIN
SPECIAL AGENT
HOMELAND SECURITY INVESTIGATIONS

The truth of the foregoing affidavit has been attested to me by Special Agent Geoffrey Goodwin over the telephone on this 1st day of March, 2024, at Bridgeport, CT.

SDV

HONORABLE S. DAVE VATTI
UNITED STATES MAGISTRATE JUDGE