

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA**

**UNITED STATES OF AMERICA,** )  
 )  
 **Plaintiff,** )  
 )  
 **v.** )  
 ) **Civil Action No. 24-cv-1667**  
 **196,721.18289916 USDT SEIZED FROM A** )  
 **BINANCE ACCOUNT HELD BY** )  
 **IZUCHUKWU HENRY OKOLO** )  
 )  
 **Defendant.** )  
 \_\_\_\_\_ )

**VERIFIED COMPLAINT FOR FORFEITURE *IN REM***

Plaintiff, the United States of America, through the U.S. Attorney for the District of Columbia, brings this verified complaint for forfeiture in a civil action *in rem* against 196,721.18289916 in Tether cryptocurrency (“USDT”), hereinafter Defendant Property, and alleges as follows:

**JURISDICTION AND VENUE**

1. This Court has original jurisdiction of this civil action by virtue of 28 U.S.C. § 1345, because it has been commenced by the United States, and by virtue of 28 U.S.C. § 1355(a), because it is an action for the recovery and enforcement of a forfeiture under an Act of Congress.
2. Venue is proper here under 18 U.S.C. § 3238 and 28 U.S.C. § 1395(a), (b), and (c).

**NATURE OF THE ACTION AND STATURY BASIS FOR FORFEITURE**

3. The United States files this *in rem* forfeiture action to seek forfeiture of Defendant Property involved in, and constituting the proceeds of, violations of wire fraud, wire fraud conspiracy, money laundering, and money laundering conspiracy activity in violation of 18 U.S.C. §§ 2, 3, 1343, 1344, 1349, 1956(a)(1)(B)(i), 1956(a)(2)(B)(i), 1956(h), and 1957.

4. 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 and 983 and the Federal Rules of Civil Procedure.

5. 18 U.S.C. § 981(a)(1)(A) mandates forfeiture of any property, real or personal, involved in a transaction or attempted transaction in violation of section 18 U.S.C. §§ 1956, 1957 or 1960, or any property traceable to such property.

6. 18 U.S.C. § 981(a)(1)(C) mandates forfeiture of property constituting or derived from proceeds traceable to wire fraud, conspiracy to commit wire fraud, bank fraud, or any offense constituting “specified unlawful activity” as defined by 18 U.S.C. § 1956(c)(7), or a conspiracy to commit such offense. A violation of 18 U.S.C. § 1343, or a conspiracy to commit that offense, and a violation of 18 U.S.C. § 1344 constitutes specified unlawful activity under 18 U.S.C. § 1956(c)(7)(A) as an offense listed in 18 U.S.C. § 1961(1)(B).

7. Title 18 U.S.C. § 1343 provides that whoever, having devised or intending to devise any 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, television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, commits the violation of wire fraud.

8. Title 18 U.S.C. § 1349 provides that whoever attempts or conspires to commit a violation of 18 U.S.C. § 1343 shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy.

9. Title 18 U.S.C. § 1344 provides that whoever knowingly executes, or attempts to execute, a scheme or artifice—to defraud a financial institution or to obtain any of the

moneys, funds, credits, assets, securities, or other property owned by, or under the custody or control of, a financial institution, b means of false or fraudulent pretenses, representations, or promises—commits the violation of bank fraud.

10. Title 18 U.S.C. § 1956(a)(1)(B)(i) provides in relevant part that whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity— . . . knowing that the transaction is designed in whole or in part . . . to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity” is guilty concealment money laundering.

11. Title 18 U.S.C. § 1956(a)(2)(B)(i) provides that whoever transports, transmits, or transfers, or attempts to transport, transmit, or transfer a monetary instrument or funds from a place in the United States to or through a place outside the United States or to a place in the United States from or through a place outside the United States—knowing that the monetary instrument or funds involved in the transportation, transmission, or transfer represent the proceeds of some form of unlawful activity and knowing that such transportation, transmission, or transfer is designed in whole or in part—to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity, commits international money laundering.

12. Title 18 U.S.C. § 1956(h) provides that any person who conspires to commit any offense of 1956 or 1957 is subject to the same penalties as those prescribed for the offense the commission of which was the object of the conspiracy.

13. Title 18 U.S.C. § 1957 provides in relevant part that “[w]hoever . . . knowingly engages or attempts to engage in a monetary transaction in criminally derived property of a value greater than \$10,000 and is derived from specified unlawful activity” is guilty of a federal offense. Because the offense consists of spending the proceeds of specified unlawful activity, section 1957 is sometimes called the “spending statute.” Violations of section 1957 are commonly referred to as money-laundering offenses.

### **PROPERTY INFORMATION**

14. The Defendant Property consists of 196,721.18289916 USDT from an account held in the name of IZUCHUKWU HENRY OKOLO (“OKOLO”).

15. The Defendant Property is currently in FBI custody and will be transferred to the United States Marshals Service in the District of Columbia.

### **STATEMENT OF FACTS**

16. The Federal Bureau of Investigation (“FBI”) seized the Defendant Property from criminals abroad involved in “pig-butcher” scams—some of whom may be victims of forced labor themselves. The United States of America seeks to lawfully forfeit the Defendant Property to punish and deter criminal activity by depriving criminals of property used in or acquired through illegal activities; to promote and enhance cooperation among federal and foreign law enforcement agencies; and most importantly: to recover assets that may be used to compensate victims.<sup>1</sup>

#### **I. Background on cryptocurrency**

17. **Virtual currency:** 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 U.S. dollar, but are generated

---

<sup>1</sup> See United States Asset Forfeiture Program, *Our Mission*, <https://www.justice.gov/afp>.

and controlled through computer software. Bitcoin (BTC) and Ether (ETH) are currently the most well-known virtual currencies in use.

18. **Stablecoins:** Stablecoins are a type of virtual currency designed to maintain a stable value relative to another asset, typically a unit of currency or commodity or basket of assets. USDT, commonly referred to as a stablecoin, is pegged to the value of the U.S. dollar, and one USDT is intended to be valued at \$1. Tether Limited is the token manager (the owner of the smart contract) and the entity responsible for keeping funds in reserve that back USDT. Tether Limited Inc. is owned by iFinex Inc., a company registered in the British Virgin Islands and reportedly headquartered in Hong Kong.

19. **Virtual currency address:** Virtual currency addresses are the specific virtual locations to or from 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.

20. **Private key:** Each virtual currency address is controlled through a unique corresponding private key, a cryptographic equivalent of a password needed to access the address. Only the holder(s) of an address's private key can authorize a transfer of virtual currency from that address to another address.

21. **Virtual currency wallet:** There are various types of virtual currency wallets, including software wallets, hardware wallets, paper wallets. A software wallet is a software application that interfaces with the virtual currency's specific blockchain and generates and stores a user's addresses and private keys. A virtual currency wallet allows users to store, send, and receive virtual currencies. A virtual currency wallet can hold many virtual currency addresses at the same time.

22. Wallets that are hosted by third parties are referred to as “hosted wallets” because the third party retains a customer’s funds until the customer is ready to transact with those funds. Conversely, wallets that allow users to exercise total, independent control over their funds are often called “unhosted” wallets.

23. **Blockchain:** The code behind many virtual currencies requires that all transactions involving that virtual currency be publicly recorded on what is known as a blockchain. The blockchain is essentially a distributed public ledger, run by a decentralized network of computers and using that blockchain’s technology, containing an immutable and historical record of every transaction. The blockchain can be updated multiple times per hour and records every virtual currency address that has ever received that virtual currency and maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies.

24. **Blockchain explorers** are online tools that operate as a blockchain search engine. Blockchain explorers enable users to search for and review transactional data for any addresses on a particular blockchain. A blockchain explorer is software that uses API and blockchain nodes to draw data from a blockchain and uses a database to arrange and present the data to a user in a searchable format.

25. **USDT**, also known as Tether, is a crypto currency that resides on multiple blockchains. The value of USDT is tied to the value of the U.S. dollar. Thus, one unit of USDT is represented to be backed by one U.S. dollar in Tether’s reserves, making it what is known as a “stablecoin.” USDT is issued by Tether Ltd. USDT is hosted on the Ethereum and Tron blockchains, among others.

26. **Ethereum (ETH)** is a cryptocurrency that is open-source and is distributed on a platform that uses “smart contract” technology. Transactions involving ETH are publicly recorded on the Ethereum blockchain, which allows anyone to track the movement of ETH.

27. **Virtual currency exchanges (VCEs)** are trading and/or storage platforms for virtual currencies such as BTC and ETH. Many VCEs also store their customers’ virtual currency in virtual currency wallets. As previously stated, these wallets can hold multiple virtual currency addresses. Because VCEs act as money services businesses, they are legally required to conduct due diligence of their customers (*i.e.*, “know your customer” or “KYC” checks) and to have anti-money laundering programs in place.

28. **Blockchain analysis:** It is virtually impossible to look at a single transaction on a blockchain and immediately ascertain the identity of the individual behind the transaction. That is because blockchain data generally consist only of alphanumeric strings and timestamps. But law enforcement can obtain leads regarding the identity of the owner of an address by analyzing blockchain data to figure out whether that same individual is connected to other relevant addresses on the blockchain. To analyze blockchain data, law enforcement can use blockchain explorers as well as commercial services offered by several different blockchain-analysis companies. These companies analyze virtual currency blockchains and attempt to identify the individuals or groups involved in transactions. “For example, when an organization creates multiple [BTC] addresses, it will often combine its [BTC] addresses into a separate, central [BTC] address (*i.e.*, a “cluster”). It is possible to identify a ‘cluster’ of [BTC] addresses held by one organization by analyzing the [BTC] blockchain’s transaction history. Open-source tools and private software products can be used to analyze a transaction.” *United States v.*

*Gratkowski*, 964 F.3d 307, 309 (5th Cir. 2020). Through numerous unrelated investigations, law enforcement has found the information provided by these tools to be reliable.

## **II. Overview of the pig-butchering scheme and related wire fraud and money laundering**

### **A. Pig-butchering defined**

29. Investment-fraud schemes are commonly referred to as “pig-butchering.” Pig-Butchering schemes begin by criminals contacting potential victims through seemingly misdirected text messages, dating applications, or professional meetup groups. Next, using various means of manipulation, the criminal gains the victim’s affection and trust. Criminals refer to victims as “pigs” at this stage because they concoct elaborate stories to “fatten up” their victims.

30. Once that trust is established, the criminal recommends cryptocurrency investment by touting their own, or an associate’s, success in the field. Means of carrying out the scheme vary, but a common tactic is to direct a victim to a fake investment platform hosted on a website. These websites, and the investment platforms hosted there, are created by criminals to mimic legitimate platforms. The subject assists the victim with opening a cryptocurrency account, often on an exchange such as Binance or Coinbase, then walks the victim through transferring money from a bank account to that cryptocurrency account. Next, the victim will receive instructions on how to transfer their cryptocurrency assets to the fake investment platform. On its surface, the platform shows lucrative returns, encouraging further investment; underneath, all deposited funds are routed to a cryptocurrency wallet address controlled completely by the criminals – the “butchering” phase of the scheme.

31. Pig-butchering perpetrators frequently allow victims to withdraw some of their “profits” early in the scheme to engender trust and help convince victims of the legitimacy of



the platform. As the scheme continues, victims are unable to withdraw their funds are provided various excuses as to why. For example, the criminals will often levy a fake “tax” requirement, stating taxes must be paid on the proceeds generated from the platform. This is just an eleventh-hour effort by the criminals to elicit more money from victims. Ultimately, victims are locked out of their accounts and lose all their funds. By using non-custodial, or “private” wallets—wallets unattributable to law enforcement by legal process or blockchain analysis alone—the comingling of victim funds, and by ensuring that victim funds transverse numerous accounts before reaching their downstream, criminals frequently transfer large sums of victim funds out of the reach of law-enforcement. To liquidate their assets, the criminals use a vast network of “brokers,” who agree to buy cryptocurrency.<sup>2</sup>

32. Based on data submitted to the FBI’s Internet Crime Complaint Center (<https://www.ic3.gov>), in 2022 alone, pig-butchering schemes targeted tens of thousands of victims in the United States and resulted in over \$2 billion in private assets being siphoned overseas.

### **B. Identification of Victim**

33. VICTIM reported to the FBI that that they were defrauded out of approximately \$1,100,000 between January 2021 and December 2022. As set forth in more detail below, the VICTIM was defrauded by one or more individual(s) purporting to be two women romantically interested in the VICTIM.

---

<sup>2</sup> Alert, Financial Crimes Enforcement Network, *FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as “Pig Butchering,”* (9/8/2023), [https://www.fincen.gov/sites/default/files/shared/FinCEN\\_Alert\\_Pig\\_Butchering\\_FINAL\\_508c.pdf](https://www.fincen.gov/sites/default/files/shared/FinCEN_Alert_Pig_Butchering_FINAL_508c.pdf).

### C. The “Markus” Scam

34. VICTIM met the first perpetrator online in December 2020 via Facebook’s dating platform. The account was in the name of Eva Markus (“Markus”) and showed pictures of a woman purported to be Markus. There was also a LinkedIn profile purporting to be Markus.

35. According to Markus’s LinkedIn page and the communications with VICTIM, Markus was an engineering consultant from Boston, Massachusetts temporarily working on a mining project in Turkey. Markus and VICTIM developed a romantic relationship communicating over the phone and via email.

36. In January 2021, Markus told VICTIM that the diamond mine she was working on exploded, she was being held responsible, and she had to hire an attorney to convince the Turkish government to let her return to the United States. From January 2021 through January 2022, Markus convinced VICTIM to send her over \$400,000 to pay her attorney and various other expenses under the guise that Markus would return to Boston as soon as she could get out of Turkey. Markus instructed VICTIM to send money through bank-to-bank wires and PayPal transactions to three individuals named Wande Cars (“Cars”), Olanrewaju Taiwo (“Taiwo”), and Cafini Z. Markus claimed that all three individuals were employees of financial institutions where she banked, and they would reroute the money to her because she could not directly access her bank accounts in Turkey. Instead, Markus told VICTIM to send money to the three individuals via separate PayPal and bank accounts.

37. Cafini Z received the bulk of the initial \$400,000 of VICTIM’s funds. Cafini Z’s LinkedIn profile notes that she lives and works in the Washington, D.C., area. Physical

surveillance of her residence in September 2022 at 3404 25<sup>th</sup> Street SE, Washington D.C. 2020 identified a vehicle registered to her parked at the address.

38. There is no indication of Cafini Z working for any financial institution. Records obtained from entities Cafini Z received or transferred VICTIM's money indicate Cafini Z claims to work as a "consultant" at Red Wheel Consulting and an "escrow agent", but her transaction activity has been flagged for being suspicious and inconsistent with escrow services. The same records indicate that Cafini Z accessed VICTIM's money on at least one occasion at a financial institution in Washington, D.C., withdrawing it in cash and converting it into cryptocurrency through at least one Bitcoin ATM located in Washington D.C. Red Wheel Consulting has no online presence, no formal business office, and no known business purpose.

39. Cars and Taiwo live in England according to the addresses they provided to open financial accounts. Similar to Cafini Z, neither Cars nor Taiwo have any known professional financial credentials.

#### **D. The "Warren" Scam**

40. VICTIM met the second woman online in April 2022, again via Facebook's dating application. The account was in the name of Lisa Warren ("Warren"). Warren offered VICTIM cryptocurrency investment services in which VICTIM could make quick profits; Warren also expressed romantic interest in VICTIM. Their relationship developed via telephone calls, texts, and emails. Warren told VICTIM that she lived in Dayton, Ohio, and claimed to work for Berox Trading ("Berox"), a company supposedly based in Coeur d'Alene, Idaho. No record of Berox was found in the Idaho Secretary of State corporate database.

41. Given Warren's advertised expertise in cryptocurrency trading and hoping to make up for the losses suffered in the Markus scam, VICTIM invested \$55,000 with Warren between April 2022 and November 2022. Per Warren's instructions, VICTIM created a Coinbase account, purchased Bitcoin, and sent the Bitcoin to a wallet Warren controlled. In December 2022, Warren told VICTIM that she was making profits on the money and that VICTIM should increase the investment. Warren convinced VICTIM to sell VICTIM's home and invest the sale proceeds with Warren via Coinbase, in the same manner as the initial \$55,000.

42. In late 2022, VICTIM repeatedly asked for the money back and to meet Warren in person. Warren returned only \$15,000 and refused to meet VICTIM in person. Warren's refusal to meet in person prompted VICTIM to travel to the address shown on Warren's driver's license, which Warren sent an image of to VICTIM in an attempt to verify her identity. Upon arrival, VICTIM asked the family living at the house if Warren was there, to which they responded they did not know Warren. Immediately thereafter, VICTIM visited the Dayton Police Department to report the scam. Dayton Police confirmed that Warren's license was fake, and Warren did not live in Ohio. As of October 2023, Warren continued to tell VICTIM the two will purchase a home together and that she is still making profits for him.

43. In total, VICTIM sent Warren \$587,197 worth of cryptocurrency including transaction and exchange fees.

44. Using records initially provided by VICTIM and, thereafter, via the blockchain public ledger, cryptocurrency exchanges, and cryptocurrency wallet addresses, the FBI has traced the Bitcoin VICTIM sent to Warren via cryptocurrency wallet bc1qpfv8gy727svexhyge20n9prtvgjqqu4nf4shq8 ("Warren's Wallet").

**E. Tracing and Freezing VICTIM's Cryptocurrency Funds**

45. As part of the investigation, the FBI has traced VICTIM's payments to both Warren and Markus. Though the approximately \$400,000 VICTIM sent to Markus in the first scam has been largely withdrawn in cash by various subjects around the world, half of the approximately \$600,000 worth of cryptocurrency VICTIM sent to Markus in the second scam has remained intact, without being extensively comingled or withdrawn.

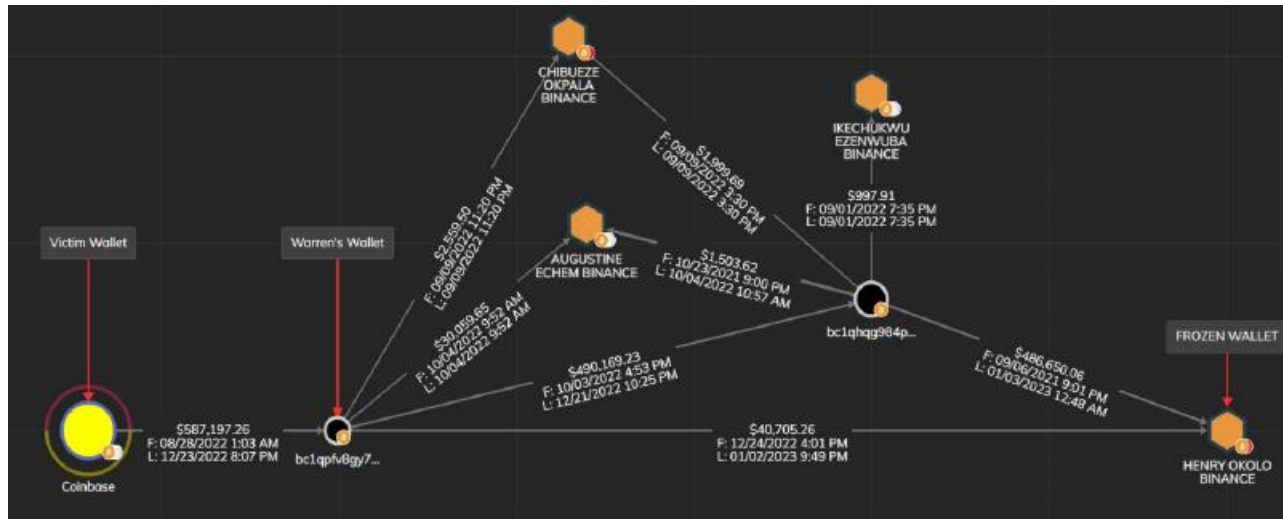
46. On November 24, 2023, 5.19678278 Bitcoin,<sup>3</sup> directly traceable back to VICTIM's Coinbase wallet 622a203a8040a185f8b38f18 ("VICTIM's Wallet") by way of Warren's Wallet, was deposited into cryptocurrency address 1B3LCA8TZEac8o5nJt46ECY3mxDWsxHkR1 held at Binance. Records received from Binance indicate that the 1B3LCA8TZEac8o5nJt46ECY3mxDWsxHkR1 address is associated with a Binance account/wallet held by Henry Okolo ("Okolo") under User ID 59011023 and registered under email address Okolohenry50@gmail.com ("Frozen Wallet"). Okolo immediately converted to 196,721 USDT, or "Tether", a cryptocurrency coin that holds value equivalent to the United States dollar. On the same date, Binance reported to the FBI that Binance froze the funds. The funds are now in custody of the FBI.

47. The FBI traced VICTIM's funds from VICTIM's Wallet to the Frozen Wallet as follows:

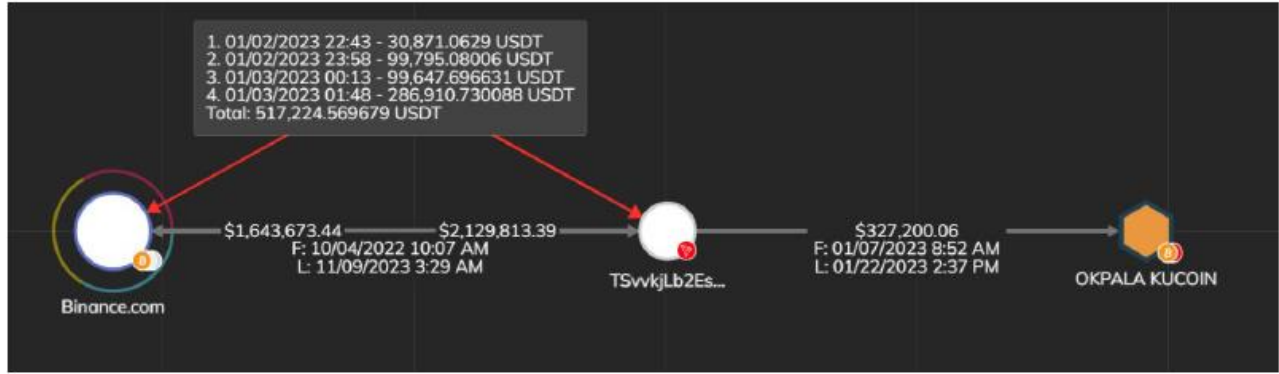
- a. As of December 23, 2022, VICTIM had sent Warren a total of \$587,197 worth of Bitcoin (approximately 34.5 Bitcoin) from VICTIM's Wallet to Warren's Wallet.

---

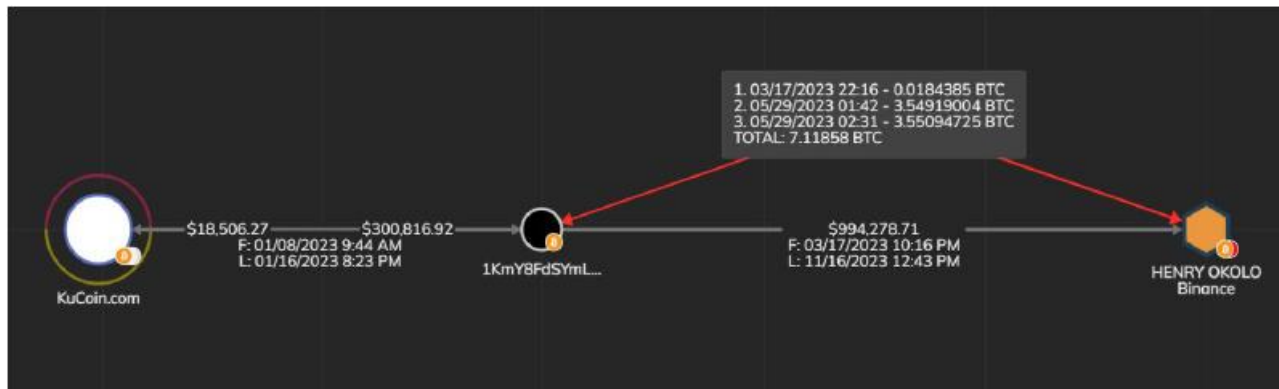
<sup>3</sup> At the time of transfer, 5.19678278 Bitcoin had a value of approximately \$216,883.



- b. From Warren's Wallet, the money was split into various wallets, with the most significant amounts going to four wallets owned individually by Chibueze Samuel Okpala, Kaodilichukwu Augustine Echem, Izuchukwu Henry Okolo, and Chinonso Ikechukwu Ezenwuba.
- c. As shown above, the vast majority of VICTIM's funds, approximately 31.64 Bitcoin (valued at approximately \$527,355.32), was sent to the Frozen Wallet.
- d. Binance records show that, upon receipt of these funds, Okolo swapped the 31.64 Bitcoin into Tether, receiving approximately 527,355.32 Tether (valued at approximately \$527,355.32).
- e. Between January 2, 2023, at 22:43 UTC, and January 3, 2023, at 01:48 UTC, Okolo transferred 517,224.57 Tether, across four transfers, from the Frozen Wallet to a private Tether address TSvvkjLb2Esnayk2xT2tCXzL7tB2xLRkJb ("TSvvkj"), where the funds remained until January 07, 2023.



f. Between January 07, 2023, and January 22, 2023, approximately 327,206.86 Tether was transferred from TSwvkj to address TQRYxu4K96ewnhiX3LXpHqqh2ZKsSGErXZ in ten transactions. The remaining 190,017.712452 Tether held in TSwvkj was not transferred. TQRYxu4K96ewnhiX3LXpHqqh2ZKsSGErXZ was later identified as a wallet owned by Okpala and held on an exchange called Kucoin as confirmed by records received from Kucoin. KuCoin records show that Okpala then exchanged the Tether for 13.84885977 Bitcoin. That Bitcoin was then sent to a private Bitcoin address, 1KmY8FdSYmLjpGi8No3N9APbVDP9YuMSxh (“1KmY”), over the course of seven transactions between January 9, 2023, and January 14, 2023.



- g. Unrelated to VICTIM's funds, law enforcement observed an additional 2.18569478 Bitcoin entered 1KmY, bringing the total Bitcoin in 1KmY to 16.03455455 Bitcoin. The Bitcoin was slowly transferred to other wallets and addresses over the following months. Due to the timing and structure of these transactions, law enforcement confirmed that the funds in 1KmY were, in fact, VICTIM's funds. Nonetheless, given the fact that VICTIM's funds were co-mingled with the additional 2.18569478 Bitcoin received by 1KmY, all of the funds described in this paragraph are assets involved in the furtherance of the money laundering scheme as they were sent and received in such a way as to obfuscate the source and ownership of the funds.
- h. Between January 2023 and May 2023, a total of approximately 7.11857579 Bitcoin was sent from 1KmY to the Frozen Wallet, split between three transactions: (1) 0.018439 Bitcoin (valued at approximately \$501.678) on or about March 17, 2023; (2) 3.54919004 Bitcoin (valued at approximately \$100,045.21) on or about May 29, 2023 at 01:42 UTC; and (3) 3.55094725 Bitcoin (valued at approximately \$100,032.28) on or about May 29, 2023, at 02:31 UTC. Law enforcement identified another 7.9175 Bitcoin sent from 1KmY to various other addresses and wallets unrelated to the Frozen Wallet.
- i. During law enforcement's analysis, the subjects were observed developing a pattern of using the Frozen Wallet as an exchange point to move VICTIM's funds to their various private wallets.
- j. This pattern continued from May 30, 2023, through at least November 16, 2023, according to records subpoenaed from Binance. Law enforcement attempted to



freeze the Frozen Wallet on multiple occasions, but the subjects moved VICTIM's funds in and out of the Frozen Wallet too fast to enact a freeze on the spot. Of note, during this time, law enforcement identified a total of approximately \$110,221.59 of various cryptocurrencies unrelated to VICTIM's funds flowed through the Frozen Wallet over twenty-one transactions. At no time were VICTIM's funds held in the Frozen Wallet during any of those twenty-one transactions.

- k. In November 2023, the FBI coordinated with Binance to set up a manual monitor on the Frozen Wallet so that Binance could monitor the activity in the Frozen Wallet and catch the stolen funds the next time the subjects passed VICTIM's funds through the Frozen Wallet.
- l. As of November 16, 2023, 5.24907093 Bitcoin was being held in the previously mentioned private wallet 1KmY.
- m. On November 24, 2023, at around 15:54 UTC, approximately 5.21244702 Bitcoin was transferred from 1KmY to private Bitcoin address 1QD1LXowhunMAJHfDSzSGuD7C7aTLwwDjj.
- n. Within two hours, at approximately 17:18 UTC, 1QD1LXowhunMAJHfDSzSGuD7C7aTLwwDjj transferred 5.21336365 Bitcoin to the Frozen Wallet, which was empty immediately prior to that deposit. Once in the Frozen Wallet, the 5.21336365 Bitcoin was exchanged for 196,721 Tether, all of which is traceable to VICTIM Wallet.

- o. On November 24, 2023, Binance alerted the FBI that VICTIM's funds – a total of 196,721 Tether – were frozen in the Frozen Wallet, which Okolo opened in 2021 and continues to control according to Binance records.
- p. Throughout 2023, law enforcement obtained Binance records for the addresses belonging to Echem, Okolo, Okpala, and Ezenwuba. "Know Your Customer" information shows Nigerian passports for Echem, Okpala, and Ezenwuba. Okolo's account does not include a Nigerian passport, but access logs predominantly show his location being Nigeria and his account phone number is a Nigerian number. All four individuals have operated their respective Binance accounts since at least 2021. There is no information indicating they are cryptocurrency investors, nor do they have any relationship with Warren.

48. Throughout 2023, law enforcement obtained Binance records for the addresses belonging to Echem, Okolo, Okpala, and Ezenwuba. "Know Your Customer" information shows Nigerian passports for Echem, Okpala, and Ezenwuba. Okolo's account does not include a Nigerian passport, but access logs predominantly show his location being Nigeria and his account phone number is a Nigerian number. All four individuals have operated their respective Binance accounts since at least 2021. There is no information indicating they are cryptocurrency investors, nor do they have any relationship with Warren.

49. There is probable cause to believe that the financial transaction involving the movement of the 5.21336365 Bitcoin from 1QD1LXowhunMAJHfDSzSGuD7C7aTLwwDjj to the Frozen Wallet, constitutes a violation of 18 U.S.C. §§ 1956(h) and 1957. Moreover, there is probable cause to believe that the Frozen Wallet contains proceeds of violations of 18

U.S.C. §§ 1343 (wire fraud), 1344 (bank fraud), and 1349 (conspiracy to commit bank fraud and wire fraud).

**Okolo's Submitted Claim**

50. After seizure, FBI provided Okolo with proper notice, allowing Okolo to submit a claim for the property. Okolo provided a sworn statement declaring “the nature of my business is simply to exchange cryptocurrencies for naira from Person to Person (P2P) and vice versa”.<sup>4</sup> Records Okolo provided with the claim show their statement to be false; one third of Okolo's order history shows USDT sold for Canadian Dollars.

51. Records obtained by law enforcement also show Okolo's claim to be false; the overwhelming amount of account activity shows Okolo, either acting alone or acting along with one or more perpetrators, transferred and received cryptocurrency between each other. The purpose of this scheme was to conceal or disguise the nature, the location, the source, the ownership, or control of the criminal proceeds.

**COUNT ONE – FORFEITURE OF DEFENDANT PROPERTY**  
**(18 U.S.C. §§ 981(a)(1)(C))**

52. Paragraphs 1 through 51 are realleged and incorporated by reference here.

53. The Defendant Funds are property constituting or derived from proceeds traceable to wire fraud and conspiracy to commit wire fraud, in violation of 18 U.S.C. §§ 1343, 1344, and 1349.

54. Accordingly, the Defendant Funds are subject to forfeiture to the United States under 18 U.S.C. § 981(a)(1)(C).

---

<sup>4</sup> Naira is the national currency of Nigeria.

**COUNT TWO – FORFEITURE OF DEFENDANT PROPERTY**

**(18 U.S.C. §§ 981(a)(1)(A))**

55. Paragraphs 1 through 51 are realleged and incorporated by reference here.

56. The Defendant funds are property involved in a transaction or attempted transaction in violation of 18 U.S.C. §§ 1956(a)(1)(B)(i), 1956(a)(2)(B)(i), 1956(h), and 1957, that is, a conspiracy to conduct or attempt to conduct financial transactions involving the proceeds of specified unlawful activity, to wit, wire fraud and conspiracy to commit wire fraud, knowing that the transaction was designed in whole and in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity, and knowing that the property involved in the financial transaction represented the proceeds of some form of unlawful activity; and a conspiracy to knowingly engage in or attempt to engage in monetary transactions in criminally derived property of a value greater than \$10,000 derived from specified unlawful activity, to wit, wire fraud and conspiracy to commit wire fraud.

57. Accordingly, the Defendant Funds are subject to forfeiture to the United States under 18 U.S.C. § 981(a)(1)(A).

**PRAYER FOR RELIEF**

WHEREFORE, the United States of America prays that notice issue on the Defendant Property as described above; that due notice be given to all parties to appear and show cause why the forfeiture should not be decreed; that this Honorable Court issue a warrant of arrest *in rem* according to law; that judgment be entered declaring that the Defendant Property be forfeited to the

United States of America for disposition according to law; and that the United States of America be granted such other relief as this Court may deem just and proper.

June 7, 2024  
Washington, D.C.

Respectfully submitted,

MATTHEW M. GRAVES  
United States Attorney  
D.C. Bar No. 481052

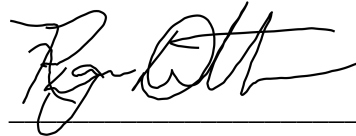
/s/ Rick Blaylock, Jr. \_\_\_\_\_

Rick Blaylock, Jr.  
TX Bar No. 24103294  
Assistant United States Attorney  
United States Attorney's Office  
601 D Street, N.W.  
Washington, D.C. 20001  
(202) 252-6765  
rick.blaylock.jr@usdoj.gov

**VERIFICATION**

I,           Ryan Dittmar          , a Special Agent with the Federal Bureau of Investigation, declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the foregoing Verified Complaint for Forfeiture *in rem* is based upon reports and information known to me and/or furnished to me by other law enforcement representatives and that everything represented herein is true and correct.

Executed on this 7th day of June 2024.

A handwritten signature in black ink, appearing to read 'Ryan Dittmar', written over a horizontal line.

Ryan Dittmar  
Special Agent  
Federal Bureau of Investigation