

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA

Plaintiff

v.

APPROXIMATELY 40,353
USDT.ETH CRYPTOCURRENCY

Defendant *in rem*

§
§
§
§
§
§
§
§
§
§
§

COMPLAINT FOR
FORFEITURE *IN REM*

CIVIL ACTION NO.
25-CV-2116

VERIFIED COMPLAINT FOR FORFEITURE IN REM

The United States of America by its attorneys, through the United States Attorney for the District of Columbia, brings this complaint for forfeiture *in rem* against approximately 20,017 USDT.ETH seized from a Binance.com account held in the name of Ehiremen Aigbokhan and 20,336 from 0xC7bdBA7ffB126F68E8454CF5e7445d3695A58c52, altogether 40,353 USDT.ETH (hereinafter referred to as the “Defendant Property”), and alleges the following:

STATEMENT OF THE CASE

1. One or more perpetrators impersonated the Trump-Vance Inaugural Committee, fraudulently stole funds from an intended donor, and then laundered the funds.
2. 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.¹

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

JURISDICTION AND VENUE

3. 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.

4. This Court has in rem jurisdiction over the Defendant Property under 28 U.S.C. §§ 1355(b) and 1395(a), (b), and (c).

5. Venue is proper in this judicial district under 18 U.S.C. §§ 3237, 3238; 28 U.S.C. §§ 1355(b); and 1395(a), (b), and (c). In this matter, a forfeiture action could be brought in the United States District Court for the District of Columbia because the criminal offenses began or were committed out of the jurisdiction of any particular State or district, and no offender is known to have, or have had, residence within any United States district. Additionally, the FBI executed a warrant for the Defendant Property in, and brought the Defendant Property to, the District of Columbia.

NATURE OF THE ACTION AND STATUTORY BASIS FOR FORFEITURE

6. The United States files this in rem forfeiture action to seek forfeiture of Defendant Property as proceeds of wire fraud, specifically 18 U.S.C. § 1343, and as involved in money laundering, and money laundering conspiracy offenses, committed in violation of 18 U.S.C. § 1956(a)(1)(B)(i) and 18 U.S.C. § 1957. 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.

7. **Wire Fraud:** 18 U.S.C. § 1343 provides in relevant part 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, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both.”

8. **Concealment Money Laundering:** 18 U.S.C. § 1956(a)(1)(B)(i) provides in relevant part that “[w]hoever, 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” shall be guilty of a federal offense. This offense is sometimes referred to as Concealment Money Laundering. The term “specified unlawful activity” is defined in 18 U.S.C. §§ 1956(c)(7) and 1961(1), and it includes violations of 18 U.S.C. § 1343 (Wire fraud).

9. **The Spending Statute:** 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” shall be guilty of a federal offense. Because the offense consists of spending the proceeds of specified unlawful activity, § 1957 is sometimes referred to as the Spending Statute. Violations of § 1957 are considered money laundering offenses.

10. **Asset Forfeiture Statute:** Pursuant to 18 U.S.C. § 981(a)(1)(C), any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of 18 U.S.C. § 1343 is subject to criminal and civil forfeiture.

11. **Asset Forfeiture Statute:** Pursuant to 18 U.S.C. § 981(a)(1)(A), any property, real or personal, which is involved in a transaction or attempted transaction in violation of sections

1956 and 1957, and/or which constitutes or is derived from proceeds traceable to wire fraud is subject to civil forfeiture.

PROPERTY INFORMATION

12. The Defendant Property consists of approximately 40,360 USDT.ETH derived from two different sources:

a. 20,017 USDT.ETH obtained from Binance.com associated with the Binance.com Account 1017886435, held in the name of Ehiremen Aigbokhan (“Aigbokhan’s Binance.com Account”); and

b. 20,336 USDT.ETH derived from an Ethereum address in an unhosted wallet, address 0xC7bdBA7ffB126F68E84554CF5e7445d3695A58c52 (“ADDRESS 58c52”), that sent USDT to Aigbokhan’s Binance.com Account.

13. The Defendant Property is currently in possession of the Federal Bureau of Investigation (“FBI”) and will be transferred to the United States Marshals Service in the District of Columbia.

STATEMENT OF FACTS

Background on Cryptocurrency and Other Definitions

14. **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 (i.e. national currencies like the dollar, euro, yen, etc.) 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. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place 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. 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.² Cryptocurrency is not illegal in the United States.

15. **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, 26–35 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. Only the holder of an address’ private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

16. Although cryptocurrencies such as bitcoin have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering and is an oft used means of payment for illegal goods and services on hidden services websites. By

² Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track transfers, trades, purchases, and other financial transactions. As of September 19, 2024, one bitcoin is worth approximately \$63,006 though the value of bitcoin is generally much more volatile than that of fiat currencies.

17. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g. Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code³ with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a "recovery seed" (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). Individuals possessing cryptocurrencies

³ A QR code is a matrix barcode that is a machine-readable optical label.

often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

18. **Cryptocurrency “exchangers” and “exchanges”** - are individuals or companies that exchange bitcoin for other currencies, including U.S. dollars. According to 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.⁴ Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and the full bank account and routing numbers that the customer links to an exchange account. As a result, there is significant market demand for illicit cryptocurrency-for-fiat currency exchangers, who lack AML or KYC protocols and often also advertise their ability to offer customers stealth and anonymity. These illicit exchangers routinely exchange fiat currency for cryptocurrencies by meeting customers in person or by shipping cash through the mail. Due to the illicit nature of these transactions and their customers’ desire for anonymity, such exchangers are frequently able to charge a higher exchange fee, often as high as 9–10% (in contrast to registered and BSA-compliant exchangers, who may charge fees as low as 1–2%).

19. **Cryptocurrency Wallet** - Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital

⁴ See “Application of FinCEN’s Regulations to Person Administering, Exchanging, or Using Virtual Currencies,” available at <https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering>.

device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), law enforcement may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

20. **Stablecoins** are a type of virtual currency whose value is pegged to a commodity's price, such as gold, or to a fiat currency, such as the U.S. dollar, or to a different virtual currency. For example, USDT is a stablecoin pegged to the U.S. dollar. Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives.

21. **Tether Limited ("Tether")** is a company that manages the smart contracts and the treasury (i.e., the funds held in reserve) for USDT tokens.

Overview of the Scheme and the Related Investigation

22. The perpetrator(s) of this scheme committed what is commonly referred to as a Business Email Compromise Scheme. In this scheme, perpetrators often send an email message

that appears to come from a known source making a legitimate request. Perpetrators slightly alter the appearance of the email address or means of communication to trick or coerce victims into providing them money. As an example, where a legitimate email address is “john.kelly@examplecompany.com,” a perpetrator may use “john.kelley@examplecompany.com.”⁵

23. In this case, the victim believed they were contributing a donation to the Trump-Vance Inaugural Committee through a false email address.

24. On December 24, 2024, the Victim (hereinafter referred to as “Victim-1”) received an email from one or more individuals purporting to be Steve Witkoff, Co-Chair of the Trump-Vance Inaugural Committee. The legitimate emails from the Trump-Vance Inaugural Committee are @t47inaugural.com, whereas the email received by Victim-1 was from @t47linaugural.com. Here, the lowercase “l” was replaced by a lowercase “L.” Depending on the font, the lowercase “L” can look like the uppercase “I.” A copy of the initial email received by Victim-1 is included below:

On Tue, Dec 24, 2024 at 3:24 PM Steve Witkoff <steve_witkoff@t47linaugural.com> wrote:

Hi Ivan & Mouna,

Please find below the USDT wallet address and barcode for the contribution:

Wallet Address: 0xC7bdBA7ffB126F68E8454CF5e7445d3695A58c52

⁵ For additional information on Business Email Compromise scams and how to protect yourself against them, see <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/business-email-compromise>.

25. The perpetrators, acting as Steve Witkoff (hereinafter “Fake Steve Witkoff”), instructed the victims to deposit funds into a cryptocurrency wallet ending in 58c52 (hereinafter “ADDRESS 58c52”).

26. Fake Steve Witkoff solicited donations from the Victim on December 24, 2024. On December 26, 2024, Victim-1 sent 250,300 USDT.ETH to ADDRESS 58c52 with the intent to and belief they were donating to the Trump-Vance Inaugural Committee. On the same date after sending their supposed donation, Victim-1 confirmed their donation in an email to the Fake Steve Witkoff, as shown in the email shown below:

----- Forwarded message -----
 From: Mouna [REDACTED]
 Date: Thu, Dec 26, 2024 at 3:47 PM
 Subject: Re: Contribution Details
 To: Steve Witkoff <steve_witkoff@t47Inaugural.com>
 CC: Ivan [REDACTED], Finance RSVP <financersvp@t47Inaugural.com>

Hi Steve- our contribution of \$250k was just processed. Here is the confirmation.
<https://etherscan.io/tx/0x74ec438cfa8f992f79fa564d38672cc247139d694fef6db6f77aca7b2485cb5>

27. The transaction details mentioned by Victim-1 in the above email, along with Etherscan,⁶ corroborate the 250,300 USDT.ETH deposit to ADDRESS 58c52. Below is a capture of the Etherscan details.

Transaction Hash:	0x74ec438cfa8f992f79fa564d38672cc247139d694fef6db6f77aca7b2485cb5
Status:	Success
Block:	21489994 27960 Block Confirmations
Timestamp:	3 days ago (Dec-26-2024 11:42:59 PM UTC) Confirmed within 11 secs
Transaction Action:	Transfer 250,300 (\$250,081.49) USDT To 0xc7bdBA7ffB126F68E8454CF5e7445d3695A58c52

⁶ Etherscan is a website that allows individuals to view addresses and transactions on the Ethereum blockchain.

28. Within approximately two hours after receiving the funds from Victim-1, records indicate funds moved from ADDRESS 58c52 to other cryptocurrency addresses. Within twenty-four hours after Victim-1 sent 250,300 USDT.ETH to ADDRESS 58c52, the perpetrator(s) transferred 215,000 USDT.ETH to numerous other cryptocurrency addresses.

29. On December 30, 2024, the FBI requested Tether to freeze the remaining USDT.ETH in ADDRESS 58c52. On or around December 31, 2024, Tether voluntarily complied with the freeze request. On December 31, 2024, at the time the freeze was effectuated, ADDRESS 58c52 contained 20,336 USDT.ETH.

30. On December 27, 2024, ADDRESS 58c52 sent 10,012 USDT.ETH to 0x2447dd599220154145a51cc750f579b015fbe386 (“ADDRESS be386”). On December 30, 2024, ADDRESS 58c52 sent an additional 10,012 USDT to ADDRESS be386.

31. On December 30, 2024, Binance.com provided records associated with ADDRESS be386. Those records indicate that on October 13, 2024, Ehiremen Aigbokhan, with an address in Lagos, Nigeria, created a Binance.com account with the User ID 1017886435. Ehiremen Aigbokhan’s Binance.com account did not receive any deposits prior to receiving the two deposits from ADDRESS 58c52. On December 30, 2024, the FBI requested Binance.com to freeze the USDT remaining in ADDRESS be386. On or about December 31, 2024, Binance.com voluntarily complied with the freeze request. On December 31, 2024, ADDRESS be386 contained approximately 20,024 USDT.ETH. On December 31, 2024, at the time the freeze was effectuated, the records from Binance.com indicated that no withdrawals were made from EHIREMEN Aigbokhan’s Binance.com account.

32. Further investigation revealed that the domain t47Lnaugural.com was created on December 15, 2024. The domain was associated with a new Microsoft user, identified by

pmmohdnajibrazak@gmail.com, and created that same day, December 15, 2024. Within two minutes of the user creation, the user created two more accounts, financiersvp@t47Lnaugural.com and steve_witkoff@t47Lnaugural.com.

33. Both financiersvp@t47Lnaugural.com and steve_witkoff@t47Lnaugural.com were accessed exclusively from Nigeria. IP geolocation data consistently showed emails from these accounts originating from Nigeria, and not the United States.

34. Logins for financiersvp@t47Lnaugural.com and steve_witkoff@t47Lnaugural.com were cross-referenced with other possible Microsoft users. One Microsoft user, ehizaza@outlook.com, also accessed the same IP addresses during the same time period as did financiersvp@t47Lnaugural.com and steve_witkoff@t47Lnaugural.com.

35. Further queries of ehizaza@outlook.com showed multiple Skype accounts associated with the email address, registered to an Ehiremen Aigbokhan. This is the same name registered on Aigbokhan's Binance account. Further details, such as addresses, emails, and birthdate, match between Binance and Microsoft.

36. Header analysis of ehizaza@outlook.com showed that emails directed to pmmohdnajibrazak@gmail.com@gmail.com and steve_witkoff@t47Lnaugural.com went to ehizaza@outlook.com's email inbox, indicating the accounts were linked. As stated before, Victim-1 transferred 250,300 USDT on December 26, 2024, on the request of Fake Steve Witkoff. Victim-1 was based in the United States. One day before and two days after the transfer, IP addresses of Aigbokhan's logins to Microsoft and Google all resolved to Lagos, Nigeria. All IP addresses from Aigbokhan's online activity that was subpoenaed, from November 2024 to January 2025, resolved to Nigeria. Therefore, it appeared likely that Aigbokhan received an international transfer of funds from the U.S. to Nigeria as a result of his fraudulent activity.

37. On January 6, 2025, the Honorable Moxila A. Upadhyaya, United States Magistrate Judge in the District of Columbia, found probable cause for seizure of the Defendant Property in seizure warrant 25-sz-1.

CONCLUSION

38. The perpetrator in this investigation fraudulently mimicked a political campaign's entity, stole funds intended for the Trump-Vance Inaugural Committee, and laundered the criminal proceeds. As such, the property is subject to forfeiture.

COUNT ONE – FORFEITURE OF DEFENDANT PROPERTY

39. The facts contained this complaint are realleged and incorporated by reference here.

40. The Defendant Property constitutes property involved in wire fraud and conspiracy to commit wire fraud in violation of 18 U.S.C § 1343.

41. Accordingly, the Defendant Property is subject to forfeiture to the United States under 18 U.S.C. § 981(a)(1)(C).

COUNT TWO – FORFEITURE OF DEFENDANT PROPERTY

42. The facts contained this complaint are realleged and incorporated by reference here.

43. The Defendant Property constitutes property involved in money laundering and conspiracy to engage in money laundering, in violation of 18 U.S.C. §§ 1956(a)(1)(B)(i) and 1957.

44. Accordingly, the Defendant Property is 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.

July 2, 2025
Washington, D.C.

Respectfully submitted,

/s/ Rick Blaylock, Jr.

Rick Blaylock, Jr.

TX Bar No. 24103294

Assistant United States Attorney

Asset Forfeiture Coordinator

United States Attorney's Office

601 D Street, N.W.

Washington, D.C. 20001

(202) 252-6765

rick.blaylock.jr@usdoj.gov

VERIFICATION

I, Alexis Brown, 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 2nd day of July 2025.



Alexis Brown
Special Agent
Federal Bureau of Investigation