IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA, Plaintiff, v. 24,273.260219 USDT TETHER (USDT) SEIZED FROM A BINANCE ACCOUNT ASSOCIATED WITH USER ID 462487648 AND EMAIL ADDRESS OSAMAIRFAN29@GMAIL.COM Defendant *in Rem.*	)	Civil Case No. 1:26-cv-00015

COMPLAINT FOR FORFEITURE IN REM

COMES NOW the plaintiff, United States of America, by and through its counsel, Lindsey Halligan, United States Attorney for the Eastern District of Virginia and Special Attorney, Todd W. Blanche, Deputy Attorney General, Robert K. McBride, First Assistant United States Attorney, and by Annie Zanobini, 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. The United States brings this action *in rem* seeking the forfeiture of all right, title and interest in the 24,273.260219 Tether (USDT) seized from a Binance Account Associated with User ID 462487648 and Email Address osamairfan29@gmail.com ("Defendant Property"). The Defendant Property is subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(C) and (a)(1)(A).

THE DEFENDANT IN REM

2. Defendant 24,273.260219 Tether (USDT) was seized from a Binance Account associated with User ID 462487648 and Email Address osamairfan29@gmail.com and is currently held in a cryptocurrency wallet address controlled by the Federal Bureau of Investigation "FBI" in the Eastern District of Virginia.

JURISDICTION AND VENUE

3. 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) and (b).

4. This Court has *in rem* jurisdiction over the Defendant Property under 28 U.S.C. § 1355(b)(1)(B) with reference to 18 U.S.C. § 1395(b) because the Defendant Property is located in the Eastern District of Virginia and under 28 U.S.C. § 1355(b)(1)(A) because acts and omissions giving rise to the forfeiture took place in the Eastern District of Virginia.

5. Venue is proper in this judicial district under 28 U.S.C. § 1355(b)(1)(B) with reference to 18 U.S.C. § 1395(b) because the Defendant Property is located in the Eastern District of Virginia and under 28 U.S.C. § 1355(b)(1)(A) because acts and omissions giving rise to the forfeiture took place in the Eastern District of Virginia.

BASIS FOR FORFEITURE

6. 18 U.S.C. § 981(a)(1)(C) provides for the forfeiture of any property, real or personal, which constitutes or is derived from proceeds traceable to any offense constituting a specified unlawful activity ("SUA"), as defined in 18 U.S.C. § 1956(c)(7), or a conspiracy to commit such SUA. 18 U.S.C. § 1956(c)(7)(A) provides that any act or activity constituting an offense under 18 U.S.C. § 1961(1) constitutes an SUA, with the exception of an act indictable

under subchapter II of Chapter 53 of Title 31 of the United States Code. 18 U.S.C. § 1961(1) references violations of 18 U.S.C. § 1343.

7. 18 U.S.C. § 981(a)(1)(A) provides for the forfeiture of any property, real or personal, involved in a violation or attempted violation of 18 U.S.C. § 1956, or any property traceable to such property.

STATEMENT OF FACTS

8. The FBI seized the Defendant Property from criminals involved in investment fraud scams. 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 and to recover assets that may be used to compensate victims.[1]

A. Background on Cryptocurrency

9. **Virtual Currency**: Virtual currencies are digital representations of value that, like traditional coin and paper currency, function as a medium of exchange (i.e., they can be digitally traded or transferred and can be used for payment or investment purposes). Virtual currencies are a type of digital asset separate and distinct from digital representations of traditional currencies, securities, and other traditional financial assets. The exchange value of a particular virtual currency generally is based on agreement or trust among its community of users. Some virtual currencies have equivalent values in real currency or can act as a substitute for real currency, while others are specific to particular virtual domains (e.g., online gaming communities) and generally cannot be exchanged for real currency. Cryptocurrencies, like Bitcoin and Ether, are types of virtual currencies, which rely on cryptography for security. Cryptocurrencies typically lack a central administrator to issue the currency and maintain

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

payment ledgers. Instead, cryptocurrencies use algorithms, a distributed ledger known as a blockchain, and a network of peer-to-peer users to maintain an accurate system of payments and receipts.

10. **Virtual Currency Address**: A virtual currency address is an alphanumeric string that designates the virtual location on a blockchain where virtual currency can be sent and received. A virtual currency address is associated with a virtual currency wallet. A virtual currency address is analogous to a bank account number.

11. **Virtual Currency Wallet:** A virtual currency 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 also allows users to send and receive virtual currencies. Multiple addresses can be stored in a wallet.

12. **Virtual Currency Exchange:** A virtual currency exchange ("VCE"), also called a cryptocurrency exchange, is a platform used to buy and sell virtual currencies. VCEs allow users to exchange their virtual currency for other virtual currencies or fiat currency, and vice versa. Many VCEs also store their customers' virtual currency addresses in hosted wallets. VCEs can be centralized (i.e., an entity or organization that facilitates virtual currency trading between parties on a large scale and often resembles traditional asset exchanges like the exchange of stocks) or decentralized (i.e., a peer-to-peer marketplace where transactions occur directly between parties).

13. **Blockchain:** Many virtual currencies publicly record their transactions on what is referred to as the "blockchain." The blockchain is essentially a distributed public ledger, run by a decentralized network, containing an immutable and historical record of every transaction that has ever occurred utilizing that blockchain's specific technology. The blockchain can be updated

multiple times per hour and records every virtual currency address that ever received that virtual currency. It also 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.

14. **Blockchain Analysis**: Although the identity of an address owner is generally anonymous (unless the owner opts to make the information publicly available), analysis of the blockchain can often be used to identify the owner of a particular address. The analysis can also, in some instances, reveal additional addresses controlled by the same individual or entity. A user of virtual currency can utilize multiple addresses at any given time and there is no limit to the number of addresses any one user can utilize.

15. **Stablecoins:** 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, USDC 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.

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

17. **Ether**: Ether ("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.

18. **Tron:** Tron ("TRX") is a cryptocurrency that is open-source and is distributed on a platform that uses "smart contract" technology. Transactions involving TRX are publicly recorded on the Tron blockchain, which allows anyone to track the movement of TRX.

19. **Bitcoin**: Bitcoin (or "BTC") is a type of virtual currency. Unlike traditional,

government-controlled currencies (i.e., fiat currencies), such as the U.S. dollar, Bitcoin is not managed or distributed by a centralized bank or entity. Because of that, Bitcoin can be traded without the need for intermediaries. Bitcoin transactions are approved/verified by computers running Bitcoin's software. Those computers are called network nodes. Each node uses cryptography to record every Bitcoin transaction on the Bitcoin blockchain. The Bitcoin blockchain is a public, distributed ledger. Bitcoin can be exchanged for fiat currency, other virtual currencies, products, and services.

B. The Investment Fraud Scheme

20. This complaint involves a fraud scheme currently being perpetrated by multiple criminal groups, both domestically and internationally. The perpetrators use a variety of schemes to trick or coerce victims, many of whom are elderly, into providing them money. Initial contact with victims is typically made with automated, previously recorded telephone calls, commonly referred to as "robocalls," that contain misleading messages that often include callback numbers for victims to contact. Once victims call the number provided, the perpetrators will offer the victims maintenance assistance with their home computers. The perpetrators attempt to convince victims that there are problems with their home computers, sometimes by tricking the victims into downloading software that the perpetrators use to create problems with the victims' computers.

21. As part of the scheme, the perpetrators send messages to create a sense of urgency by telling the victim that if they did not fix the problem with their computer there would be drastic financial consequences. The fraudsters will instruct the victim that, in order to prevent these dire consequences, the victim needs to withdraw money from their bank and deposit it into a "secure ATM" which ends up being a cryptocurrency ATM.

3. The Victim

22. On or about January 31, 2025, the victim, a female residing in Herndon, Virginia, within the Eastern District of Virginia, received a pop-up notification on the victim's laptop computer which indicated that the computer had been compromised. The victim subsequently called the provided telephone number, purportedly for Microsoft. The victim was instructed to download an application in order to clean the computer. The scammer guided the victim through multiple steps to clean the computer. The scammer also notified the victim that there was suspicious activity on their credit cards and checking account. The scammer provided the victim a case number and connected the victim with the Bank of America fraud department. The second scammer, purportedly from Bank of America, informed the victim that someone had authorized release of $39,000 from the victim's checking account, but that the scammer had put a hold on the transaction.

23. The scammer then told the victim that the bank branch had multiple problems and that someone inside the bank had authorized it. Therefore, in order to keep the money safe, the victim was instructed to go to the bank, withdraw $25,000, and put the cash in a secure ATM. On or about January 31, 2025, the victim drove to the victim's bank, withdrew $20,000, and then drove to a Bitcoin ATM located in Herndon, VA, and made two cash deposits of $10,000 each to said Bitcoin ATM. The victim was then instructed to return home and call Scammer 2—who was represented to be a Bank of America representative. While on the phone with Scammer 2, the victim received an official-looking document from the FDIC which acknowledged their receipt of the victim's first two $10,000 deposits, provided the victim with a Bank of America case number with the FTC, a contact phone number for the FTC and FDIC, and, urged the victim to keep these matters to herself until advised by the FDIC or Bank Fraud

Analyst, which Scammer 2 reinforced to the victim on the phone. On or about February 1, 2025, the victim received a call from Scammer 3 who stated that the victim's computer was fine and that he would have the Bank of America person contact the victim.

24. On or about February 1, 2025, Scammer 4 instructed the victim to travel to a different Bank of America branch to withdraw $22,000. The victim then made a cash deposit of $22,000 at a Bitcoin ATM located in Herndon, VA. Scammer 4 then instructed the victim to travel to a third Bank of America branch to withdraw $25,000. Upon requesting the withdrawal, the bank manager spoke to the victim and informed the victim that she was likely the victim of a scam, because Bank of America does not handle fraud in this manner. The victim later contacted Bank of America to freeze the victim's accounts and on or about February 3, 2025, the victim filed a complaint with the FBI's Internet Crime Complaint Center (IC3).

25. On or about April 10, 2025, the victim provided the FBI with photographs of the receipts for the above-referenced cash deposits into the cryptocurrency ATMs. The receipts indicated that the victim's first deposit was for $10,000 in cash, resulting in 0.06980542 BTC (after fees) being deposited into BTC address 1LNutfdzrr3JWohWH8L6c1rQbh36ozzv2f ("zv2f") on or about January 31, 2025. The victim's second deposit was for $10,000 in cash, resulting in 0.06960799 BTC (after fees) being deposited into BTC address zv2f on or about January 31, 2025. Lastly, the victim's third deposit was for $22,000 in cash, resulting in 0.15406162 BTC (after fees) being deposited into BTC address bc1qm4m046eI02g9a907m6d3x4dtsxmt2scm95tlls ("bc1qm4") on or about February 1, 2025.

D. Post-Theft Movement of Funds

26. Investigators used blockchain analysis to trace the victim's stolen funds following the above-described transactions, in which the victim sent a total of approximately 0.29347503 BTC.[2]

27. Blockchain analysis was performed on the initial two deposits of about $10,000, resulting in the transfer of around 0.13941341 to zv2f. The analysis revealed that the entirety of these funds was eventually transferred to three addresses: 3KYL1jDixS149bheiRPBRAbnLSbt6J9fVB, 3DqutLtu1Z8t8ih5qwxLTSxNsrrfX85ADV, and 36M8t7mozCsWUB5H5ACpVEQswqBNeG899C, all of which are associated with accounts at KuCoin, a cryptocurrency exchange.

28. On or about February 1, 2025, the victim completed her third transaction by depositing approximately $22,000 USD into an Athena Bitcoin ATM Kiosk, #21769, located on Elden St, in Herndon, VA. This deposit resulted in the purchase and transfer of 0.15406162 BTC, valued at about $15,714.05,[3] which was transferred to bc1qm4 on or about February 1, 2025, at around 17:03. This is the first transaction that bc1qm4 had ever received, and therefore held a balance of 0 BTC prior to this transfer.

29. Approximately 15 minutes later, at around 17:18, bc1qm4 transferred approximately 0.15405823 BTC to 1nYyc25uYH8vGABe27gZDTv9iMPhiqMQ4 (1NYyc). Blockchain analysis indicates that 1nYyc is a bitcoin address associated with an account held at Binance.com, a cryptocurrency exchange.

---

[2] *See* ¶ 41 for visual representation of the flow of funds described herein.

[3] Cryptocurrency Kiosks (ATM's)frequently have extremely high usage fees, which are borne by the individuals depositing cash into the kiosk. These high fees explain the discrepancy between the value of cash deposited ($22,000) and the value of the BTC purchased ($15,714.05), with the remainder of $6,285.95 being taken by the Cryptocurrency Kiosk as a usage fee.

30. On or about February 5, 2025, law enforcement requested account records from Binance for the account associated with 1nYyc. Binance records indicate that 1nYyc is associated with Binance account XXXX3194, registered to P.N., an Indian national. Prior to the above-described deposit, this account had received approximately $4,334.85544940 worth of cryptocurrency in the form of BTC, ETH, and USDT, and withdrawn approximately $4,385.99911978 worth of cryptocurrency, in the form of ETH and USDT, to various addresses, effectively bringing the balance of the account to 0.

31. Following the receipt of the 0.15405823 BTC into Binance Account 207983194, on or about February 1, 2025, at about 17:25:55, the BTC was almost immediately swapped to approximately 15780.2980136 USDT on the Tron network. Minutes later, at approximately 17:27:10, 15,734.343306 USDT was withdrawn from Binance Account 207983194, and sent to an unhosted USDT address, TJBsGM5B4Bv5UUgrb9h7cZGCrvdionNCEF (TJBs).

32. Prior to this transaction, on or about February 1, 2025, TJBs held a balance of approximately 52,633.7506 USDT. Following the deposit, the balance was brought to approximately 68,368.0939 USDT on or about February 1, 2025 at around 17:27. Between 17:17 and 18:30, TJBs conducted one outgoing transaction of approximately 10 USDT, and received approximately four deposits of about 669.451096 unrelated USDT, bringing the balance to 69,027.545 USDT as of 18:30. At around 18:45 and 18:56, TJBs conducted two outgoing transactions, sending 10,000 and 58,000 USDT to address TQrddKBgKQZdq1w58LAnRJ3ZCiLVP5PzSE (TQrd).

33. Prior to this transaction, on or about February 1, 2025, TQrd held a balance of approximately 2,521.150032 USDT. Upon the receipt of both above-described transactions, on or about February 1, 2025, at around 18:56, TQrd's balance was brought to approximately

70,521.15003. Following this, TQrd conducted one outgoing transaction of approximately -1,835 USDT at around 19:44 and another, totaling approximately 605 USDT, at around 21:01, bringing the balance of TQrd to approximately 68,081.15003 USDT. Minutes later, at around 21:13, TQrd sent an outgoing transaction of approximately 60,000 USDT to address THVJWAVaeSvgMXsTyr2bT195MkWNoJBZ7p (THVJ).

34. Prior to this transaction, on or about February 1, 2025, THVJ held a balance of approximately 171,808.1659 USDT. Upon the receipt of the above-described transaction, on or about February 1, 2025, at around 21:13, THVJ's balance was brought to approximately 231,808.1659. The next transaction, on or about February 2, 2025, at around 14:08, THVJ transferred approximately -48,518 USDT to TBJJJGgNBs8tFNEMMMfTAF6BiYAftSGdMT (TBJJ). Blockchain analysis indicates that TBJJis a Tron address associated with an account held at Binance.

35. Binance records indicate that TBJJ is associated with Binance account 462487648, registered to Usama Irfan Irfan Elahi, with email address osamairfan29@gmail.com, a Pakistani national residing in the United Arab Emirates ("Binance Account 462487648"). Prior to the above-described deposit, this account had received approximately $11,725.89595233 worth of cryptocurrency in the form of USDC, ETH, and USDT, and had withdrawn approximately $11,110.53785240 worth of cryptocurrency, in the form of SOL, BNB, ETH and USDT, to various addresses. This account had not received a deposit or made an outgoing withdrawal since around January 16, 2025.

36. Following the deposit of 48,518 USDT into Binance Account 462487648**,** the USDT was then swapped for various cryptocurrencies, including LDO, SOL, XRP, and ETH. Of this, between about 02/03/2025 and 02/04/2025, the majority of the USDT was swapped to

ETH, resulting in the swap of approximately 42,156.74216177 USDT for approximately 15 ETH (14.9968 ETH, valued at around $43,189.13).

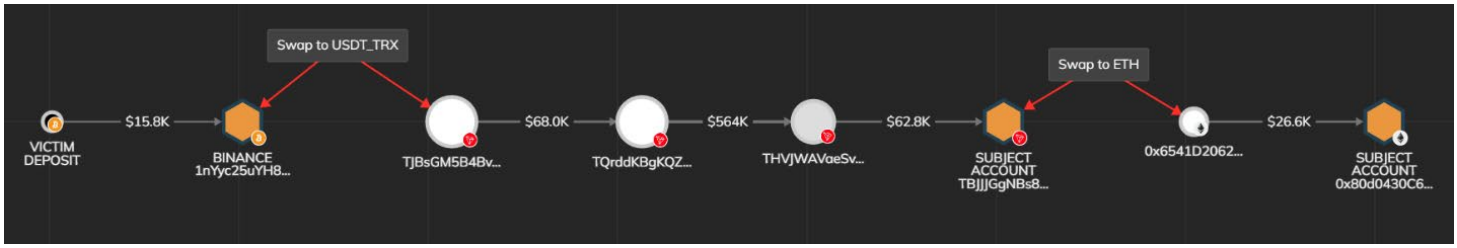
37. A series of convoluted transactions and quick swaps from one type of cryptocurrency to another is a strong indication that the movement of funds was performed in a manner meant to conceal the nature, source, control, and/or ownership of the proceeds of a specified unlawful activity, to wit, wire fraud.

38. Starting on or about February 4, 2025, Binance Account 462487648 began withdrawing these cryptocurrencies. On or about February 4, 2025, at around 00:26:53, Binance Account 462487648 withdrew approximately 0.9984 ETH, valued at around $2,875.28, and transferred it to address 0x6541D20627F448C35e9bB2A25E61bE4eEea1D249 (0x65). About two minutes later, at around 00:28:36, Binance Account 462487648 withdrew an additional approximately 13.9984 ETH, valued at about $ 40,313.85, and transferred it to 0x65.

39. Prior to this transaction, on or about February 4, 2025, 0x65 held a balance of approximately 0.00442 ETH. Following the deposit of the two above transactions, the balance of 0x65 was 15.00122 ETH. This cryptocurrency remained in 0x65 for approximately two months, during which period 0x65 did not conduct any incoming or outgoing transactions.

40. On or about April 6, 2025, at around 13:55, 0x65 transferred approximately 0.028417565239159907 ETH, valued at around $50.48, to 0x80d0430C69864B1d9F058DAa98688351be498831 (0x80). 0x80 is an ETH address that is associated with Binance Account 462487648. Minutes later, at around 13:58, 0x65 transferred approximately 14.972725460428984093 ETH, valued at around $26,597.99, to Binance Account 462487648 at the 0x80 address.

41. A visual representation of the flow of funds is below:



42. The Binance records indicated that, as of April 7, 2025, Binance Account 462487648 held a balance of approximately 25,110.3174384435 USDT, valued at around $25,110.32. Prior to the above-described transfers, Binance Account 462487648 had not received incoming transactions since on or about February 25, 2025, and made no outgoing transactions since on or about March 13, 2025. On or about April 7, 2025, at around 08:43:54, Binance Account 462487648 converted the approximately 15.001117 ETH received from 0x65 into approximately 14,475.04506272 XRP. About an hour later, at around 09:16:57, Binance Account 462487648 converted the about 14,475.04506272 XRP into around 25,110.31745671 USDT, valued at around $25,110.32.

43. On or about April 10, 2025, Binance confirmed that a freeze was placed on Binance Account 462487648. As of April 10, 2025, Binance Account 462487648 held a balance of approximately 24,275.66021774 USDT, valued at around $24,275.66. Binance Account 462487648 had received no additional deposits; however, Binance Account 462487648 had made a small number of trades resulting in a small loss, and subsequently transferred the remaining 24,275.66021774, valued at around $24,275.66, into Binance Account 462487648's Futures Wallet. Therefore, financial tracing of Binance Account 462487648 using the lowest intermediate balance rule indicates that the majority of the frozen funds are indeed victim funds.

44. The movement of the funds since the victim's initial deposit into the Cryptocurrency Kiosk, to their current whereabouts in Binance Account 462487648, is indicative of common typologies and techniques used to launder funds. It is highly atypical for funds not involved in money laundering to systematically and routinely be swapped at all, let alone by using two separate and completely unrelated cryptocurrency exchange accounts controlled by individuals in two different countries.

45. Attempting to convert cryptocurrency multiple times, and then holding cryptocurrency in unhosted addresses for extended periods of time, is an additional indicator of money laundering. By keeping the funds out of an exchange and stopping the movement of funds, actors hope to avoid detection by law enforcement either through concealment or the simple passage of time.

46. On or about June 6, 2025, the FBI obtained and served a lawful seizure warrant for the contents of Binance Account 462487648. At the time that the warrant was served, the account balance of Binance Account 462487648 was approximately 24,275.66021774 USDT.

47. On or about July 1, 2025, Binance transferred 18.8 USDT to a FBI-controlled Cryptocurrency Wallet.

48. On or about July 9, 2025, Binance transferred the remaining balance, 24,254.460219, to the same FBI-controlled cryptocurrency wallet, bringing the total balance to 24,273.260219 USDT. Each of the above-described transactions from Binance Account 462487648 to the FBI-controlled cryptocurrency wallet incurred a small fee, which explains the approximately 2.39999874 USDT difference between the amount frozen in Binance Account 462487648 and the amount received in the FBI-controlled wallet.

FIRST CLAIM FOR RELIEF
(Forfeiture under 18 U.S.C. § 981(a)(1)(A))

49. The United States incorporates by reference paragraphs 1–48 above as if fully set forth herein. Title 18, United States Code, Section 981(a)(1)(A) subjects to forfeiture "[a]ny property, real or personal, involved in a transaction or attempted transaction in violation of section 1956 . . . of this title, or any property traceable to such property."

50. Title 18, United States Code, Section 1956(a)(1)(B)(i) imposes criminal liability on "[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."

51. As set forth above, the Defendant Property constitutes property involved in a violation of section 1956.

52. As such, the Defendant Property is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(A).

SECOND CLAIM FOR RELIEF
(Forfeiture under 18 U.S.C. § 981(a)(1)(C))

53. The United States incorporates by reference paragraphs 1–48 above as if fully set forth herein.

54. Title 18, United States Code, Section 981(a)(1)(C) subjects to forfeiture "[a]ny property, real or personal, which constitutes or is derived from proceeds traceable to . . . any offense constituting 'specified unlawful activity' (as defined in section 1956(c)(7) of this title) or a conspiracy to commit such offense."

55. Title 18, United States Code, Section 1343 imposes a criminal penalty on any person who:

> 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…

56. Title 18, United States Code, Section 1956(c)(7)(A) provides that the term "specified unlawful activity" includes "any act or activity constituting an offense listed in section 1961(1) of this title." Title 18, United States Code, Section 1961(1) lists "any act which is indictable under any of the following provisions of title 18, United States Code. . . section 1343 (relating to wire fraud)."

57. As set forth above, the Defendant Property constitutes criminal proceeds of the wire fraud scheme.

58. As such, the Defendant Property is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C).

PRAYER FOR RELIEF

WHEREFORE, the United States prays that due process issue to enforce the forfeiture of the Defendant Property and that due notice be given to all interested parties to appear and show cause why said forfeiture of the Defendant Property should not be decreed, that the Defendant Property be condemned and forfeited to the United States to be disposed of according to law, and for such other and further relief as this Honorable Court may deem just and proper.

DATED this 2nd day of January 2026.

Respectfully submitted,

LINDSEY HALLIGAN
UNITED STATES ATTORNEY & SPECIAL ATTORNEY

TODD W. BLANCHE
DEPUTY ATTORNEY GENERAL

ROBERT K. MCBRIDE
FIRST ASSISTANT UNITED STATES ATTORNEY

By: _/s/Annie Zanobini_____
Annie Zanobini
Assistant United States Attorney
California Bar No. 321324
2100 Jamieson Avenue
Alexandria, Virginia 22314
Office Number: (703) 299-3903
Facsimile Number: (703) 299-3982
Email Address: annie.zanobini2@usdoj.gov

VERIFICATION

I, Michael Imbler, Special Agent with the Federal Bureau of Investigation, declare under penalty of perjury as provided by 28 U.S.C. § 1746, that the foregoing Complaint for Forfeiture in Rem is based on information known by me personally and/or furnished to me by various federal, state, and local law enforcement agencies, and that everything contained herein is true and correct to the best of my knowledge.

Executed at _Manassas , Virginia, this __2__of January, 2026

Michael Imbler, Special Agent
Federal Bureau of Investigation