

UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	
	)	Civil Action No. 25-cv-173
APPROXIMATELY 942,462.845 USDT,	)	
	)	
Defendant.	)	
_____	)	

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

Plaintiff, the United States of America, by and through the United States Attorney for the District of Columbia and the Assistant Attorney General for the National Security Division, brings this verified complaint for forfeiture in a civil action *in rem* against approximately 942,462.845 USDT, hereinafter the “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).

**STATUTORY AUTHORITY**

**Offense Statutes**

3. This investigation relates to violations of 18 U.S.C. § 1028 (Identity theft), 18 U.S.C. § 1030 (Computer fraud and abuse), 18 U.S.C. § 1343 (Wire fraud), 18 U.S.C. § 1956 (Money laundering), and conspiracy to commit the foregoing offenses in violation of 18 U.S.C. §§ 371, 1349, and 1956(h).

4. **Identity theft:** 18 U.S.C. § 1028(a)(1) makes it a crime, *inter alia*, to knowingly and without lawful authority produce an identification document, authentication feature, or a false identification document. 18 U.S.C. § 1028(a)(7) makes it a crime, *inter alia*, to knowingly transfer, possess, or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law. The term “means of identification” is defined in 18 U.S.C. § 1028(d)(7) and includes, *inter alia*, name, social security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.

5. **Computer fraud and abuse:** 18 U.S.C. § 1030(a)(2)(C) makes it a crime, *inter alia*, to intentionally access a computer without authorization and thereby obtain information from any protected computer. 18 U.S.C. § 1030(a)(4) makes it a crime, *inter alia*, to knowingly and with intent to defraud, access a protected computer without authorization, and by means of such conduct further the intended fraud and obtain anything of value. The term “protected computer” is defined in 18 U.S.C. § 1030(e)(2) and includes, *inter alia*, a computer used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States. *See Van Buren v. United States*, 141 S. Ct. 1648, 1652 (2021) (definition of protected computer under 18 U.S.C. § 1030(e)(2)(B) includes “at a minimum . . . all computers that connect to the Internet”).

6. 18 U.S.C. § 371 prohibits a conspiracy to commit an offense or to defraud the United States, including violations of 18 U.S.C. § 1028(a)(7) and 1030(a)(2).

7. **Wire fraud:** 18 U.S.C. § 1343 makes it a crime for anyone, 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, to transmit or cause 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. 18 U.S.C. § 1349 prohibits the attempt or conspiracy of a violation of 18 U.S.C. § 1343.

8. **Money laundering:** 18 U.S.C. § 1956(a)(1)(A)(i) makes it a crime to conduct or attempt to conduct a financial transaction, knowing that the property involved in the transaction represents the proceeds of some form of unlawful activity, and which in fact involves the proceeds of specified unlawful activity, with the intent to promote the carrying on of specified unlawful activity. This offense is sometimes referred to as promotional money laundering. 18 U.S.C. § 1956(a)(1)(B)(i) makes it a crime to conduct or attempt to conduct a financial transaction, knowing that the property involved in the transaction represents the proceeds of some form of unlawful activity, and 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. This offense is sometimes referred to as concealment money laundering.

9. 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. § 1030 (Computer fraud and abuse) and 18 U.S.C. § 1343 (Wire fraud).

10. 18 U.S.C. § 1956(h) criminalizes a conspiracy to violate § 1956.

#### **Forfeiture Statutes**

11. Pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c), any property, real or personal, which constitutes or is derived from “proceeds” traceable to a violation of 18 U.S.C. § 1030

(Computer fraud and abuse), 18 U.S.C. § 1343 (Wire fraud), or a conspiracy to commit such offenses, is subject to criminal and civil forfeiture.

12. Pursuant to 18 U.S.C. § 982(a)(1) and 18 U.S.C. § 981(a)(1)(A), any property, real or personal, “involved in” a transaction or attempted transaction in violation of 18 U.S.C. § 1956 (Money laundering) is subject to criminal and civil forfeiture. Forfeiture pursuant to these statutes applies to more than just the proceeds of the crime. These forfeitures encompass all property “involved in” the crime or the attempted crime, which can include “clean” or “legitimate” money that is commingled with “tainted” money derived from illicit sources. This commingling is a laundering technique that facilitates the scheme because it obfuscates the trail of the illicit funds. *See, e.g., United States v. Huber*, 404 F.3d 1047, 1058 (8th Cir. 2005) (the presence of legitimate funds does not make a money laundering transaction lawful; it is only necessary to show that the transaction involves criminal proceeds); *United States v. Bikundi*, 125 F. Supp. 3d 178, 194 (D.D.C. 2015) (even “otherwise untainted money may become ‘involved’ in a money laundering offense” for these purposes “where those funds are comingled with illicit proceeds” and “the government produces evidence that the legitimate funds were used to conceal the source of illicit proceeds.”)

13. 18 U.S.C. § 981(b) states that property subject to forfeiture under Section 981 may be seized via a civil seizure warrant issued by a judicial officer “in any district in which a forfeiture action against the property may be filed,” and may be executed “in any district in which the property is found,” if there is probable cause to believe the property is subject to forfeiture. 18 U.S.C. § 982(b)(1) incorporates the procedures in 21 U.S.C. § 853 (other than subsection (d)) for all stages of a criminal forfeiture proceeding. Section 853 permits the government to request the issuance of a seizure warrant for property subject to criminal forfeiture. Seizures are appropriate from this district, because the criminal offenses under investigation were begun or committed upon the high seas, or

elsewhere 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. *See* 18 U.S.C. § 3238.

### **DEFINITIONS**

14. **Virtual Currency**: Virtual currencies are digital tokens of value circulated over the Internet. Virtual currencies are typically not issued by any government or bank like traditional fiat currencies, such as the U.S. dollar, but rather are generated and controlled through computer software. Different virtual currencies operate on different blockchains, and there are many different, widely used virtual currencies currently in circulation. Bitcoin (or BTC) and ether (ETH) are currently the most well-known virtual currencies in use. BTC exists on the Bitcoin blockchain, and ETH exists on the Ethereum network. Typically, a virtual currency that is “native” to a particular blockchain cannot be used on a different blockchain. Thus, absent technological solutions those native assets are siloed within a specific blockchain. For instance, ETH (the native token on the Ethereum network) cannot be used on other networks unless it is “wrapped” by smart contract code.

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. Stablecoins achieve their price stability via collateralizations (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives.

16. **Tether (USDT)**: Tether Limited is a company that manages the smart contracts and the treasury (*i.e.*, the funds held in reserve) for USDT, a stablecoin pegged to the U.S. dollar.

17. **USD Coin (USDC)**: Circle Internet Financial Limited (“Circle”) is a company that manages the smart contracts and the treasury (*i.e.*, the funds held in reserve) for USDC, a stablecoin pegged to the U.S. dollar.

18. **Virtual Currency Address**: Virtual currency addresses are the particular virtual locations to which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of letters and numbers.

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

20. **Virtual Currency Wallet**: There are various types of virtual currency wallets, including software wallets, hardware wallets, and paper wallets. The virtual currency wallets at issue for the purposes of this affidavit are software wallets (*i.e.*, 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.

21. 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.

22. **Blockchain**: Many virtual currencies publicly record all of their transactions on what is known as a blockchain. The blockchain is essentially a distributed public ledger, run by the decentralized network of computers, containing an immutable and historical record of every transaction utilizing that blockchain's technology. 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.

23. **Blockchain Explorer**: These explorers are online tools that operate as a blockchain search engine allowing users the ability to search for and review transactional data for any addresses on a particular blockchain. A blockchain explorer is software that uses application programming interface (“API”)<sup>1</sup> 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.

24. **Smart Contracts**: Smart contracts are computer programs stored on a blockchain that run when predetermined conditions are met. Typically, they are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary’s involvement. The Ethereum network is designed and functions based on smart contracts.

25. **Virtual Currency Bridge**: A blockchain bridge, otherwise known as a cross-chain bridge, connects two blockchains and allows users to send virtual currency from one chain to the other.

26. **Virtual Currency Exchanges (VCEs)**: VCEs are trading and/or storage platforms for virtual currencies, such as BTC and ETH. There are generally two types of VCEs: centralized exchanges and decentralized exchanges, which are also known as “DEXs.” Many VCEs also store their customers’ virtual currency in virtual currency wallets. As previously stated, these wallets can hold multiple virtual currency addresses associated with a user on a VCE’s network. Because VCEs act as money services businesses, they are legally required to conduct due diligence of their

---

<sup>1</sup> API is an initialism for “application programming interface,” which is a set of definitions and protocols for building and integrating application software.

customers (i.e., KYC checks) and to have anti-money laundering programs in place (to the extent they operate and service customers in the United States).

27. **Virtual Currency Mixers:** Virtual currency mixers (also known as tumblers or mixing services) are software services that allow users, for a fee, to send virtual currency to designated recipients in a manner designed to conceal and obfuscate the source of the virtual currency. Virtual currency mixers are a common laundering tool used by North Korean cyber actors and their money laundering co-conspirators.

28. **Blockchain Analysis:** As previously stated, while the identity of a virtual currency address owner is generally anonymous, law enforcement can identify the owner of a particular virtual currency address by analyzing the blockchain (e.g., the Bitcoin blockchain). The analysis can also reveal additional addresses controlled by the same individual or entity. “[W]hen 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).

29. In addition to using publicly available blockchain explorers, law enforcement uses commercial services offered by several different blockchain-analysis companies to investigate virtual currency transactions. These companies analyze virtual currency blockchains and attempt to identify the individuals or groups involved in transactions. Through numerous unrelated investigations, law enforcement has found the information provided by these tools to be reliable.

30. **Decentralized Finance (DeFi):** Decentralized Finance, or DeFi, is an umbrella term for financial services on public blockchains, primarily the Ethereum network. The Ethereum



network's native virtual currency is ETH. Ethereum was the first blockchain that offered various decentralized services within its network. To make these services possible, the Ethereum network allows other tokens besides ETH to run within the network. These tokens are known as ERC-20 tokens.

31. DeFi is a term used to describe a financial system that operates without the need for traditional, centralized intermediaries. Instead, DeFi platforms offer an alternative financial system that is open for anyone to use, and that allows centralized intermediaries to be replaced by decentralized applications (or dApps). With DeFi, one can do most of the things that banks support—earn interest, borrow, lend, buy insurance, trade derivatives, trade assets, etc.—but it is faster than using traditional banks and does not require paperwork or a third party. DeFi is global, peer-to-peer (*i.e.*, directly between two people rather than routed through a centralized system), pseudonymous, and open to the public.

32. **Instant Exchange:** Instant exchanges are non-custodial exchanges that typically support a wide variety of currency types and convert funds immediately. All users need to do is enter the trade they want to make and the order is filled immediately.

## **STATEMENT OF FACTS**

### **Background on North Korean Information Technology Workers**

33. The Federal Bureau of Investigation (“FBI”) is investigating several recent virtual currency heists perpetrated by known and suspected Democratic People’s Republic of Korea (“DPRK” or “North Korea”) information technology (“IT”) workers who use false identities to gain employment—typically remote employment—as developers, among other jobs, with virtual currency companies and then subsequently exploit these companies’ smart contracts to steal funds.

This includes the March 29, 2024, theft of approximately \$950,000 dollars' worth of virtual currency from users of an application offered by U.S. Company 1,<sup>2</sup> as further described below.

34. In May 2022, the United States Government issued a Public Service Announcement describing this type of scheme.<sup>3</sup> In sum, the North Korean regime has dispatched thousands of highly skilled IT workers around the world to countries other than the United States to generate revenue that contributes to its weapons of mass destruction, ballistic missile, and cyber programs. These IT workers accomplish this fraud by posing as non-North Korean nationals through identity theft and the assistance of co-conspirators located around the world, including in the United States. IT workers use these personas to gain remote employment with companies, including virtual currency platforms, and then funnel payments back to the regime. IT workers regularly use U.S.-based computer infrastructure to create persona accounts. IT workers sometimes use their privileged access to victim company networks/U.S.-based computer infrastructure for illicit purposes, such as stealing cryptocurrency and enabling or conducting malicious cyber intrusions.

35. The FBI attributed the U.S. Company 1 theft to North Korean IT workers based on, among other things, distinctive tactics, techniques, and procedures observed in this heist and other virtual currency heists linked to North Korea IT workers. For example, the FBI has observed North Korea actors using Internet Protocol (IP) addresses hosted by the Russian telecommunications company TransTeleCom (TTK) service in other North Korea IT worker investigations. According to open-source information, the North Korean government began leasing internet access from TTK in or about October 2017; TTK is assigned autonomous system (AS) 20485. In the other IT worker

---

<sup>2</sup> U.S. Company 1 is no longer in business.

<sup>3</sup> See the joint Department of Treasury, Department of State, and Federal Bureau of Investigation Fact Sheet dated May 16, 2022, which is available here: <https://ofac.treasury.gov/media/923131/download?inline>.

investigations, TTK IP addresses associated with AS 20485 have been observed logging into command-and-control servers, logging into operational accounts, and conducting spear phishing attacks. In this case, as described in greater detail below, a TTK IP addresses assigned AS 20485 initiated the transfer of stolen funds from users of the U.S. Company 1 to threat-actor-controlled wallets.

### **Summary of the U.S. Company 1 Heist**

36. U.S. Company 1 was a DeFi application for trading the Solana virtual currency via a trading bot. A trading bot is software that is programmed to automatically buy and sell virtual currency based on pre-determined market parameters. Trading bots have direct access to users' virtual currency wallets in order to make trades on behalf of the users. In this case, users sent and received information from the U.S. Company 1 trading bot through the Telegram messaging application. Users needed to grant the U.S. Company 1 trading bot access to their virtual currency wallets in order for the bot to withdraw virtual currency for the purpose of conducting trades.

37. On or about March 29, 2024, North Korean actors stole approximately 6,045 Solana from the users of U.S. Company 1. The virtual currency stolen from those users was laundered through multiple unhosted wallets before being sent through several centralized exchanges, including HTX.com, Binance, MEXC.com, and FixedFloat, which moved the value of the virtual currency from one blockchain to another. The use of rapid wallet transfers and exchanges in this fashion is a money laundering technique used to obfuscate the true source of these transactions. The virtual currency was then sent through FixedFloat, an instant exchange, to the accounts and addresses that comprise the Defendant Property.

38. The Defendant Property represents funds traceable to the March 2024 exploit and theft of funds from U.S. Company 1's users.

**U.S. Company 1 Heist and Tracing of Funds**

39. On or about March 29, 2024, U.S. Company 1 suffered an exploit resulting in the compromise of its users' private keys. According to a trusted source, on or about March 29, 2024, U.S. Company 1 users, including several based in the United States, reported on X that their Solana wallets had been accessed without authorization and depleted of funds. The source attributed the theft to North Korean IT workers who had worked for U.S. Company 1.

40. Further investigation revealed the attackers leveraged access to the private keys of another previously compromised trading bot to access the U.S. Company 1 users' wallets without authorization and initiate transfers of funds out of U.S. Company 1. (U.S. Company 1 users had imported this previously compromised trading bot to U.S. Company 1, unwittingly introducing a vulnerability.) Over 400 U.S. Company 1 users had approximately 6,045 Solana (SOL) stolen from their cryptocurrency addresses, resulting in a total loss valued at approximately \$1 million, as of the time of the theft. U.S. Company 1 shut down its business shortly after the theft.

41. The same day the compromise was reported, March 29, the North Korean actors moved the SOL from the victims' wallets to 32 threat-actor-controlled wallets. The transfers from the victim wallets to the threat-actor-controlled wallets were conducted in a short period of time and were initiated from the TTK IP address 83.234.227.29. Based on the information provided by the source and the known use of TTK-supplied IP addresses by the North Korean government, the FBI assesses the theft was likely perpetrated by North Korean actors.

42. On March 31, 2024, all of the funds from the 32 threat-actor-controlled wallet addresses were then sent to several instant exchanges, including FixedFloat and EasyBit, where the SOL was converted to USDT on the Ethereum blockchain. The majority of the SOL was consolidated at the following FixedFloat deposit address:

5ndLnEYqSFIA5yUFHo6LVZ1eWc6Rhh11K5CfJNkoHEPs (“5ndLnEY”). The funds consolidated at 5ndLnEY were received from 22 of the 32 threat-actor-controlled wallets. Each of the threat-actor-controlled wallets sent the funds through a single intermediary address before depositing the funds into 5ndLnEY.<sup>4</sup>

43. The threat actors then swapped the SOL for Tether (USDT) and Ether (ETH) and moved the USDT and ETH from 5ndLnEY to the following addresses:

0x84Ad3Ad89CC96e82EE1D57151fDbDcaA823e6aCc	(“Defendant Property 1”)
0xD7AD5a1db7739C01d9B4471c5B9ffb871F625941	(“Defendant Property 2”)
0x05ae4747262f351eC861355987E8ED58a78F10Ca	(“Defendant Property 3”)
0x6a0012bdDdA0bC958c28691b373f6236e8fAbAa0	(“Defendant Property 4”)
0xC955915bd7fa544D26d5Bb6547A8169CB37130C4	(“Defendant Property 5”)
0x5e6BA75E0FbDc9a9dd0fbDEe5d4B0bfEAC9f0Fb6	(“Defendant Property 6”)
0x9A9fd8435a02CB1Dc4c8F5Db33f31aA5C56CA3e7	(“Defendant Property 7”)
0xA4436a1D19fd53275817D38b5282b9c3951599E	(“Defendant Property 8”)
0x99caa2DD9f1f845a9a01422c991c472d15ceD1d1	(“Defendant Property 9”)
0x474604bcfa36FDf518bECFcaEBB0C98b5B85A152	(“Defendant Property 10”)
0x8E2eb468D10e53f99639f02D58a19aB3d60cd07d	(“Defendant Property 11”)
0x1DBbD7182Ee17720d09121c20bc658De28F2054F	(“Defendant Property 12”)
0x6bE0873C769Cb4E9Fb3CD42Fa25bC179945cd2b9	(“Defendant Property 13”)
0xd4aC8325131512D792EeadD73B694B744dE9D947	(“Defendant Property 14”)
0x71E8aB7C141A58bd79948c11C9d8D1F7ef041F47	(“Defendant Property 15”)
0xB86369eD3754a404C5C0D5AA9Da6400A9466053E	(“Defendant Property 16”)
0x0A9Ed2a9d3F811B3cd6aD673CDEcCd88047618CA	(“Defendant Property 17”)
0x1C7F7F7b66d1f6e9C23545c0156A6A1F676C0E1b	(“Defendant Property 18”)
0x284512d226465443e04ffFE82FA20628a94D46B6	(“Defendant Property 19”)
0x48CFaFE2460570575e80eaCD4f762c7cF8F6f3B3	(“Defendant Property 20”)
0x655113606AAFe1549dcCfeD4E120DA22b6CddA24	(“Defendant Property 21”)
0xDdb5DEd6c513747b8B831d7521E00c3202Bc08fd	(“Defendant Property 22”)
0x97BeCBB90ff30513e7984e3bdcE4863d03d59FC4	(“Defendant Property 23”)
0x05C8A416aE8dB42B737a15c4C3FF5F5beF051FEf	(“Defendant Property 24”)

<sup>4</sup> The remaining assets—which are not the subject of this Complaint for Forfeiture in rem—were split, with approximately 243 SOL sent to HTX.com and approximately 1,124 SOL sent to Binance, where the actors converted the SOL to ETH and transferred the ETH through four intermediary wallets into MEXC.com, a virtual currency exchange. As of May 5, 2024, the North Korean actors had logged in ten times to the threat-actor-controlled MEXC account from IP address 83.234.227.29, the TTK IP address.

44. The above addresses are the Defendant Property. At the request of law enforcement, Tether voluntarily froze the Defendant Property, and as a result, the USDT associated with the Defendant Property. In total, the frozen USDT amounts to 942,462.845 USDT, as of March 30, 2024.

45. On or about May 31, 2024, the FBI seized the Defendant Property. All of the funds were transferred into an FBI-controlled virtual currency wallet. As of December 2024, the balance in the government-controlled wallet was 942,462.845 USDT.

46. The Defendant Property remains in the possession of the FBI; this Verified Complaint for Forfeiture *In Rem* pertains to the 942,462.845 USDT seized from Tether, as described above.

**COUNT ONE – FORFEITURE OF DEFENDANT PROPERTY**

**(18 U.S.C. §§ 981(a)(1)(C) & 28 U.S.C. § 2461(c))**

47. Paragraphs 1 through 46 are realleged and incorporated herein by reference.

48. The Defendant Property is property constituting or derived from proceeds traceable to identity theft, computer fraud, wire fraud, and conspiracy to commit computer fraud and wire fraud, in violation of 18 U.S.C. §§ 1028, 1030, 1343, 1349 and 371.

49. Accordingly, the Defendant Property is subject to forfeiture to the United States under 18 U.S.C. § 981(a)(1)(C) & 28 U.S.C. § 2461(c).

**COUNT TWO – FORFEITURE OF DEFENDANT PROPERTY**

**(18 U.S.C. § 981(a)(1)(A))**

50. Paragraphs 1 through 48 are realleged and incorporated herein by reference.

51. The Defendant Property is property involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956(a)(1)(B)(i) and 1956(h), that is, a conspiracy to conduct or attempt to conduct financial transactions involving the proceeds of specified unlawful activity, to wit, computer fraud, wire fraud, conspiracy to commit computer 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.

52. 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.

January 21, 2025  
Washington, D.C.

Respectfully submitted,

DEVIN DEBACKER  
Acting Assistant Attorney General  
National Security Division  
U.S. Department of Justice

SEAN M. NEWELL  
Chief, National Security Cyber Section  
National Security Division  
U.S. Department of Justice

EDWARD R. MARTIN, JR.  
Acting United States Attorney  
D.C. Bar No. 481866

By: /s/ Gregory Jon Nicosia, Jr.  
GREGORY JON NICOSIA, JR.  
D.C. Bar No. 1033923  
Trial Attorney  
National Security Cyber Section  
National Security Division  
U.S. Department of Justice  
D.C. Bar No. 1033923  
950 Pennsylvania Avenue NW  
Washington, D.C. 20530  
Telephone: 202-353-4273

/s/ Thomas N. Saunders  
THOMAS N. SAUNDERS  
N.Y. Bar No. 4876975  
Assistant United States Attorney  
National Security Section  
United States Attorney's Office  
601 D Street, N.W.  
Washington, D.C. 20001  
(202) 252-7790


/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



**VERIFICATION**

I, Zachary Hampton, 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 21 day of January 2025.



A handwritten signature in black ink, appearing to be 'ZAH', is written over a horizontal line. The signature is fluid and cursive.

Zachary Hampton  
Special Agent  
Federal Bureau of Investigation