UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	
	)	**Civil Action No. 25-cv-2555**
APPROXIMATELY 1,008,902.606307 USDT,	)	
	)	
Defendant.	)	
	)	

VERIFIED COMPLAINT FOR FORFEITURE *IN REM*

Plaintiff, the United States of America, by and through the U.S. 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 1,008,902.606307 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. § 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. Pursuant to 18 U.S.C. § 1030(i), "any property, real or personal, constituting or derived from, any proceeds . . . obtained" in violation of 18 U.S.C. 1030 is subject to criminal forfeiture.

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")[1] 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 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

[1] API is an initialism for "application programming interface," which is a set of definitions and protocols for building and integrating application software.

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.

STATEMENT OF FACTS

Background on North Korean Information Technology Workers

30. 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 theft of approximately $1.4 million dollars' worth of virtual currency from Company 1 in or around August 2024, as further described below.

31. In May 2022, the United States Government issued an advisory describing this type of scheme.[2] 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. The IT workers use these personas to gain remote employment with companies, including virtual currency platforms, and then funnel payments back to the regime. The IT workers regularly use U.S.-based computer infrastructure to create persona accounts. The IT workers sometimes use their privileged access to victim company networks/U.S.-based computer infrastructure for illicit purposes, such as stealing virtual currency and enabling or conducting malicious cyber intrusions.

32. The FBI attributed the 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. Specifically, one of the North Korean IT workers obtained remote employment under false pretenses as a blockchain developer to gain access to Company 1's private key, followed by laundering of the stolen funds through several exchanges, swapping currencies or value to different blockchains, to make following those assets more difficult and to prevent stolen funds from being frozen by law enforcement, as described in detail below.

[2] Department of Treasury, Department of State, and Federal Bureau of Investigation, *Fact Sheet: Guidance on the Democratic People's Republic of Korea Information Technology Workers* (May 16, 2022), https://ofac.treasury.gov/media/923131/download?inline.

Summary of the Company 1 Heist

33. Company 1 is a U.S.-based company headquartered in New York. In or about August 2024, Company 1 filed an Internet Crimes Complaint Center ("IC3") complaint stating it was a victim of North Korean IT workers and that virtual currency valued at approximately $1,350,000 was stolen from its cryptocurrency wallet 7ANPW36t8LekXXS1jACir59RGvnCAacxKFH9Zq6tW4UZ ("7ANPW3"). This theft occurred in three transactions.

34. In or about December 2024, the FBI interviewed Company 1 regarding the IC3 complaint. Company 1 told the FBI that Company 1 wanted to create a way for individuals to interact with non-fungible tokens ("NFTs") in the same way they interacted with computer files. In furtherance of these goals, Company 1 began developing a mobile application that allowed clients to purchase cryptocurrencies on various blockchains.

35. On or about December 2022, Company 1 hired Bong Chee Shen ("SHEN") as a full stack developer to assist with the company's online development and blockchain needs. A full stack developer is a computer programmer who has a high level of competency in both frontend and backend computer programming languages. Company 1 identified SHEN via an NFT community on Discord. Discord is an online platform where members can communicate, collaborate, and share information in real-time via text, voice, and video.

36. As part of his job role, SHEN was Company 1's primary cryptocurrency wallet engineer and had access to the wallet keys that managed Company 1's wallet ("7ANPW3"). After being hired, SHEN recommended two other individuals to Company 1, Joshua Charles Palmer ("PALMER") and Chris Yu ("YU"), stating he had worked with them both on previous projects. Company 1 hired both PALMER and YU as developers based upon this recommendation.

37. In or about May 2024, Company 1 terminated SHEN, PALMER, and YU due to poor performance. In addition to poor performance, Company 1 told the FBI that all three former employees had issues being able to communicate on calls and frequent issues with their microphones not working.

38. In early August 2024, Company 1 noted that all of the funds in their multi-signature wallet (which consisted of Company 1's treasury funds) had been drained of virtual currency valued at approximately $1,350,000 in three separate transactions. The theft involved three unauthorized transfers from Company 1's wallet ("7ANPW3") to wallet 6USfQ9BX33LNvuR44TXr8XKzyEgervPcF4QtZZfWMnet ("6USfQ9BX").

39. Company 1 told the FBI, that, as part of its response to the theft, Company 1 was able to identify within the wallet infrastructure a vulnerability that had been created by SHEN. This vulnerability was related to the storing of the private key associated with the company wallet. Company 1 also told the FBI that it had hired an online cryptocurrency investigator to assist in the company's investigation of the theft. The investigator specialized in tracking blockchain transactions, exposing fraudulent schemes, and helping victims recover funds. At the conclusion of the investigation, the investigator advised Company 1 that it had hired DPRK IT workers who were using fake identities.

40. In connection with his application to Company 1, SHEN provided Company 1 with an image of a Malaysia Identification Card, with an identification number ending in -6221. An image of the Malaysia Identification Card provided by SHEN is shown below:

Figure 1: Bong Chee Shen Malysia Identification Card

"Bong Chee Shen"

41. The FBI has identified the persona Bong Chee Shen as being a fraudulent online persona used to obtain remote IT developer positions.

42. In 2022, a blockchain research and development company (Company 2) headquartered in Atlanta, Georgia, told the FBI that virtual currency valued at over $700,000 had been stolen from Company 2. Company 2 told the FBI it had hired a developer who worked remotely. The developer used his access at Company 2 to transfer virtual currency valued at over $700,000 to a virtual currency address he controlled. Company 2 subsequently learned that the developer had used fictitious identity information to obtain employment with the company.

43. The FBI's tracing of the stolen funds from Company 2 identified multiple wallets used to facilitate transfers of the funds. The FBI determined the Bong Chee Shen persona, and the associated Malysia Identification Card (Figure 1), was presented as Know-Your-Customer information for one of these wallets at a virtual currency exchange. The FBI determined that the identification card was fraudulent, and that Chang Nam Il, a North Korean citizen, used the Bong Chee Shen persona and the identification card to open an account at that virtual currency exchange. On June 24, 2025, Chang Nam Il and three North Korean co-conspirators were indicted by a grand jury in the United States District Court for the Northern District of Georgia for, *inter alia*, wire fraud

conspiracy and money laundering conspiracy, in violation of 18 U.S.C. §§ 1349 and 1956(h), respectively, for their roles in the theft and laundering of virtual currency from Company 2 and another virtual currency company.

"Joshua Charles Palmer"

44. As stated above, after SHEN was hired by Company 1, SHEN stated that he had worked with PALMER on previous projects and recommended Company 1 hire him. Company 1 subsequently hired PALMER as a remote developer.

45. In connection with his application, PALMER provided Company 1 with an image of a Michigan Identification Card. A photo of the Michigan Identification Card provided by PALMER is shown below:

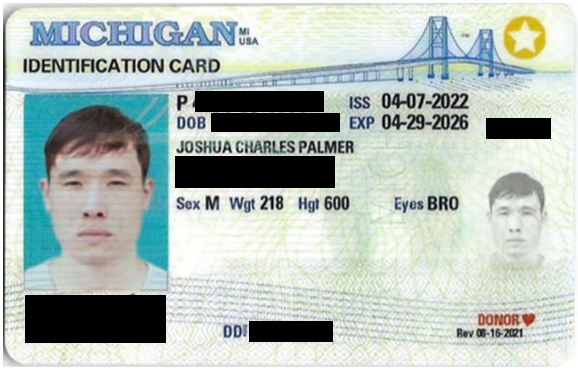

Figure 2: Counterfeit Joshua Charles Palmer Identification Card

46. According to the Michigan Department of Motor Vehicles ("DMV"), a Michigan Driver's License was issued on April 7, 2022, to an individual named Joshua Charles Palmer bearing the same serial number as the number in the Michigan Identification Card that PALMER provided to Company 1. The photograph of Joshua Charles Palmer maintained by the Michigan DMV bears no resemblance to the individual depicted in Figure 2, above.

"Chris Yu"

47. As stated above, after SHEN was hired by Company 1, SHEN stated that he had worked with YU on previous projects and recommended Company 1 hire him. Company 1 subsequently hired YU as a remote developer.

48. In connection to his application to Company 1, YU provided Company 1 with an image of a Malaysia passport. The passport was issued to Chris Yu, with a birth year of 1992, and the place of birth listed as Kuala Lumpur. An image of the Malaysia passport provided by YU is shown below:

Figure 3: Malaysia passport for YU

49. According to information provided to the FBI, the name "Chris Yu," located in Kuala Lumpur, Malaysia, is associated with DRPK IT workers.

Tracing Company 1's Funds to the Defendant Property

50. On or about August 7, 2024, North Korean actors and/or their money laundering co-conspirators (NKAs) began a series of unauthorized transfers from the Company 1 wallet 7ANPW3. The transactions were as follows:

a. On or about August 7, 2024, at 13:10 UTC on the Solana blockchain, the NKAs transferred 796,698.064613 USDC from Company 1 wallet 7ANPW3 to NKA-

controlled wallet 6USfQ9BX in transaction hash BDDHFgZP4jQwJN5viXqPUjRW6Upubq3U6DscAZ3nzJW9iKNnmcdRvjsvaUrZBTMnixwnSdc3zuxd8SAZyHpvyXe.

b. On or about August 7, 2024, at 13:29 UTC on the Solana blockchain, the NKAs transferred 1,445.238572751 SOL from Company 1 wallet 7ANPW3 to NKA-controlled wallet 6USfQ9BX in transaction hash 22DCjz4Z8kFQCt4VM1qJaXTb6V9UY3GqWpD4s2A3s88SHRerAj3kQhbGopbbHWUBAiZY2WuraTGwHYczXoqNosXo.

c. On or about August 7, 2024, at 13:47 UTC on the Solana blockchain, the NKAs transferred 1,315.82568576 SOL from Company 1 wallet 7ANPW3 to NKA-controlled wallet 6USfQ9BX in transaction hash 2tpN34QKjbNjZKc2AmdQ4t9FxAkCodFP5z7B7CeHXKhddB9Yyu4JzLCwGSuEhimPPH4FnXhytzoUsvx6DwXyLngk.

51. After making these three initial transfers into 6USfQ9BX, the NKAs began a multi-step laundering process designed to obscure the movement of assets and cryptocurrency conversions across the Solana blockchain into the Ethereum blockchain through the deBridge Finance Protocol. The resulting withdrawal addresses on the Ethereum blockchain were 0xb713a396ce6a62df4c7c857d974f4a331bde1e03 ("0xb713a3") and 0x27553f77d9d3ddf8e936c9cc00c2db6018edade4 ("0x27553f"), as described in the paragraphs below:

a. On or about August 9, 2024, at 14:05 UTC, the NKAs transferred 100 ETH from wallet 0xb713a3 to wallet 0x9e4b887772060e35254fd53363d89effd4715ec5

("0x9e4b88") in transaction hash 0x94d345a5b0d60b209ef592efbf706e6614cd69ad953874f2dd612c54374cd1f0.

b. On or about August 9, 2024, at 14:44 UTC, the NKAs transferred 254.54152876567704 ETH from wallet 0xb713a3 to wallet 0xe47eeb1d64f0a9eb9a670946723d538c5515a80e ("0xe47eeb") in transaction hash 0x2debe6c198f3d557c1dced5c4bec492ca17c75790ffa8732064e42cf482d1c2c.

c. On or about August 9, 2024, at 12:42 UTC, the NKAs transferred 149.31027549926782 ETH from wallet 0x27553f to wallet 0x9e4b88 in transaction hash 0xabe6911d69c3fb3665157cf154c9c3172bc07d051eb45035ff9aca941e29fe89.

d. On or about August 9, 2024, at 15:34 UTC, the NKAs transferred 199.07788756833946 ETH from wallet 0x9e4b88 to wallet 0xe47eeb in transaction hash 0x208fb334ddf8ba143c912d8a121b3639d7a277c51f13b85bb496675d1a34fc05.

e. On or about August 10, 2024, at 07:44 UTC, the NKAs transferred 452.7193412910367 ETH from wallet 0xe47eeb to wallet 0xde6e9a059f7930a9561a551d13bf95c4a1d519b4 ("0xde6e9a") in transaction hash 0x20a0231fb446ba35e6d0b99c6c9a01e58d4e19f32ccf36ef0ee856ed7fd017a6.

f. On or about August 10, 2024, at 08:55 UTC, the NKAs transferred 453.7193044826234 ETH from wallet 0xde6e9a to wallet 0x93d310827047da2652e1b4537d7f45d8d8bf0c3d ("0x93d310") in transaction hash 0x1080873c9c9410f15983db261a6e9438218e4c0109f299865456a9a8fc8febbf.

g. On or about August 13, 2024, at 18:19 UTC, the NKAs transferred 332.7190285560428 ETH from wallet 0x93d310 to wallet

0x4c2f93ae9bba83da0b061df78df33d98bb1f45c5 ("0x4c2f93") in transaction 0xa5be8bab24fb701bccbb23f578901103e755d884bd98157348611bee34f12573.

h. On or about August 20, 2024, at 11:19 UTC, the NKAs transferred 332.7188743157868 ETH from wallet 0x4c2f93 to wallet 0x1de7301761ac60c07e4acb3645eed81d06c57fb5 ("0x1de730") in transaction hash 0xf271ecb288c3b27f2a1afc84af81d6cd2ee7944f648f007a5a07a860c60c7413.

i. On or about November 19, 2024, at 09:44 UTC, the NKAs transferred 332.7186016956888 ETH from wallet 0x1de730 to wallet 0xb0655c92bf75f63254ec70d7c1086e0f325b29de ("0xb0655c") in transaction hash 0x20d77b9efe0deac7ef4c45af5a9b442eb5c0947d3532f52483b1f25b220ecfad.

52. On November 19, 2024, at 10:23 UTC, the NKAs converted and transferred 300,000 USDT from wallet 0xb0655c to wallet 0x66b37234b9cf5a7fbbda45076e70164962dc7c8d ("Defendant Property") in transaction hash 0x230f3932940d0c49200875f517d8cf6a16b283ecb87af58e4e03ea9b9734f254.

53. On November 19, 2024, at 10:51 UTC, the NKAs converted and transferred 300,000 USDT from wallet 0xb0655c to the Defendant Property in transaction hash 0xaa81953861f952b3d84d338f36bc14fd28749a7dabdea76e9dee71a9944164c5.

54. On November 19, 2024, at 11:05 UTC, the NKAs converted and transferred 400,000 USDT from wallet 0xb0655c to the Defendant Property in transaction hash 0x973ef1a80d9255e8bf8377dcc57c1d580819181d07855041eb2196cfd3bee7d5.

55. As of this writing, the balance for the Defendant Property consists of 1,008,902.606307 USDT.

56. On or about April 17, 2025, the FBI served Tether Limited with a warrant to seize the Defendant Property, and Tether Limited effectuated the transfer of the above funds into an FBI-controlled virtual currency wallet on or about July 17, 2025.

57. The Defendant Property remains in the possession of the FBI; this Verified Complaint for Forfeiture *In Rem* pertains only to the 1,008,902.606307 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))

58. Paragraphs 1 through 57 are realleged and incorporated herein by reference.

59. 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.

60. 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))

61. Paragraphs 1 through 57 are realleged and incorporated herein by reference.

62. 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.

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

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.

August 5, 2025
Washington, D.C.

Respectfully submitted,

JOHN A. EISENBERG
Assistant Attorney General
National Security Division
U.S. Department of Justice

JEANINE FERRIS PIRRO
United States Attorney for the District of Columbia

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
Assistant United States Attorney
N.Y. Bar No. 4876975
National Security Section
601 D Street, NW, Room 5-120
Washington, D.C. 20530
Office: 202-252-7790
Email: thomas.saunders@usdoj.gov

/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, Derek Trout, 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 5th day of August 2025.

Derek Trout
Special Agent
Federal Bureau of Investigation