UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	
	)	**Civil Action No. 25-cv-** 1769
VIRTUAL CURRENCY ASSOCIATED WITH NORTH KOREAN IT WORKER MONEY LAUNDERING AND SANCTIONS EVASION CONSPIRACIES,	)	
	)	
Defendant.	)	
	)	

VERIFIED COMPLAINT FOR FORFEITURE *IN REM*

Plaintiff, the United States of America, through the U.S. Attorney for the District of Columbia, brings this verified complaint for forfeiture in a civil action *in rem* against "Defendant Property," as defined and described below, and alleges as follows:

NATURE OF THE ACTION

1. As described below, this is a civil forfeiture action brought pursuant to 18 U.S.C. § 981(a)(1)(A) and (C) against virtual currency, nonfungible tokens (NFTs), and Ethereum Name Service (ENS) domains, all of which were involved in a conspiracy (or multiple conspiracies) to violate 18 U.S.C. § 1956(a)(2)(A) and 18 U.S.C. §§ 1956(a)(1)(A)(i) and (B)(i), all in violation of 18 U.S.C. § 1956(h), and which constituted the proceeds of wire fraud in violation of 18 U.S.C. § 1343, and of violations of the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. § 1701, *et. seq.*[1]

[1] All dates, times, and amounts referenced in this document are approximate.

THE DEFENDANTS *IN REM*

2. The defendants *in rem* are as follows:

a. Virtual currency seized from unhosted[2] virtual currency addresses and two accounts at Binance (a virtual currency exchange or "VCE") during the execution of seizure warrant 22-sz-6 (collectively referred to herein as the "March 2022 Seized Property"):

Unhosted Address Assets	**Amount**
BTC	0.0088168900
LTC	0.1277800100
ETH	521.8746883372
STARL	29692425251.2506000000
ENS	9356.0348458065
USDT	57108.4877230000
DBUY	3496980.1704557400
KUMA	138831744207.6800000000
USDC	11408.4319970000
CRV	2701.7377850068
DAI	3547.2432407695
SMI	239599819.0021540000
PERP	4.6601186800
GTC	0.0000449293
BNB	1.6022037064
BUSD	6750.0000000000
ABGRT	0.5760000000
MATIC	9.9860082833
FTM	16.8386154779
AVAX	2.8160756402

Binance Account 81090004:	
BNB	0.0000124000
BTC	0.0000073300
ETH	145.7000897500

[2] As explained below, an unhosted wallet, also known as a self-hosted or non-custodial wallet, is a virtual currency wallet through which the user has complete control over storing and securing their private keys and virtual currency. All of the unhosted wallet addresses from which law enforcement seized funds tied to this investigation are listed, in full, in Attachment A.

USDT	1484636.8067804600
SAND	14082.9700000000
USDC	0.7433070000
BUSD	0.4068787400

<u>Binance Account 118543589:</u>

BNB	0.0000521300
ETH	0.0000350000
USDT	2411417.7593996300

b. Virtual currency seized from unhosted virtual currency addresses, NFTs, and ENS domain names during the execution of seizure warrant 22-sz-13 (collectively referred to herein as the "June 2022 Seized Property"):

<u>Unhosted Address Assets</u>	**<u>Amount</u>**
Punk Vault (NFTX)	0.135126
USD Coin (USDC)	1,668.782899
SafeMoon Inu (SMI)	264,222,552.086639
UniCrypt (UNCX)	3.000000
Ethereum (ETH)	0.192765
Tether (USDT)	77.122725
Project Inverse (XIV)	3,000.000000

<u>NFTs:</u>
"Tender Morphism" 7/7
Gurlz Go Wildd #43
"Sweet Symphony" 10/10
Invisible Scissors #15
Invisible Scissors #86
Invisible Scissors #35

<u>ENS Domain Names:</u>
vhurryharry.eth
halfmooneye.eth

c. Virtual currency seized from two accounts at Binance during the execution of seizure warrant 22-sz-18 (collectively referred to herein as the "August 2022 Seized Property"):

Binance Account 369902286:

Asset	**Amount**
BTC	1.047995
USDT	200

Binance Account 126474093:

Asset	**Amount**
USDT	135

d. Virtual currency seized from unhosted virtual currency addresses 0x815F335f976301f496167bfeF237f0622F92ac38 and 0x81c4d8816b29147c542dDE87485608204690Acf2 during the execution of seizure warrant 22-sz-19 (collectively referred to herein as the "September 2022 Seized Property"):

Asset	**Amount**
USDC on Ethereum	187,035.41
USDC on Avalanche	31,584.20
USDC on Ethereum	12,262.25

e. Virtual currency in the form of USDT (a stablecoin pegged to the U.S. dollar) that was voluntarily frozen by Tether Limited ("Tether," the company that mints/creates USDT tokens) on or about September 1, 2022, in unhosted virtual currency addresses 0x815F335f976301f496167bfeF237f0622F92ac38 and 0x81c4d8816b29147c542dDE87485608204690Acf2 (i.e., the same addresses referenced above in paragraph 2(d), as virtual currency addresses can store more than one type of virtual currency at a time):

Asset	**Amount**
USDT on Ethereum	145,491.97
USDT on Ethereum	387,550.90

f. USDT that was voluntarily frozen by Tether on or about March 6, 2023, in unhosted virtual currency address 0x4F47Bc496083C727c5fbe3CE9CDf2B0f6496270c.

g. USDT that was voluntarily frozen by Tether on or about March 6, 2023, in unhosted virtual currency addresses 0x5707aA6944E357cEa1A25Ff991fB3A2E60268AB5 and 0xB389B4B4a8a6E267CA0712321cdca5c856ef8A72.

h. USDT that was voluntarily frozen by Tether on or about April 1, 2023, in unhosted virtual currency addresses 0x15824de78A61a8B493CCd8A48e58463536B17028, 0x6E2F0deAB1C358547b353342524489e32640D530, 0x3E24F610639e105173003EF1c47dC4DbAa33f8D7, and 0x1c097e02bCd6cD69946663ace4bc0B115e256bAc.

3. All of the items above are also listed in Attachment A and are collectively referred to herein as the "Defendant Property."

JURISDICTION AND VENUE

4. Plaintiff brings this action *in rem* to forfeit and condemn the Defendant Property. This Court has jurisdiction over an action commenced by the United States under 28 U.S.C. § 1345, over an action for forfeiture under 28 U.S.C. § 1355(a), and over this particular action under 18 U.S.C. § 981(a)(1)(A) and (C).

5. This Court has *in rem* jurisdiction over the Defendant Property under 28 U.S.C. § 1355(b). Upon the filing of this complaint, the plaintiff requests that the Court issue an arrest warrant *in rem* pursuant to Supplemental Rule G(3)(b), which the plaintiff will execute upon the Defendant Property pursuant to 28 U.S.C. § 1355(d) and Supplemental Rule G(3)(C).

6. Venue is proper in this district pursuant to 28 U.S.C. § 1355(b)(1)(A) because one or more of the acts or omissions in furtherance of the conspiracy or conspiracies giving rise to the forfeiture occurred in this district. That is, in sending, attempting to send, and conspiring to send funds from a place in the United States to or through a place outside the United States, or to a place in the United States from or through a place outside the United States, as a means of evading sanctions placed on North Korea, and without obtaining a license to do so from the Office of Foreign Assets Control ("OFAC"), which is located in the District of Columbia, the persons who sent, attempted to send, and conspired to send said funds committed an act or omission in this district. Venue is this district is also appropriate under 28 U.S.C. § 1355(b)(1)(B) and 18 U.S.C. § 3238 because the conspiracy or conspiracies giving rise to the forfeiture began and was committed outside the United States, and no prospective defendant is known to have resided in the United States. Venue in this district is also appropriate under 28 U.S.C. § 1395(a) as the accrues in this district, (b) as the property may be found in this district, and (c) as the government seized the property outside any judicial district and brought it to this district.

BASIS FOR FORFEITURE

7. The Defendant Property is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A) because it is property that was involved in violations of, and a conspiracy, or multiple conspiracies, to violate several provisions of the money laundering statute, including violations of 18 U.S.C. §§ 1956(a)(1)(A)(i), (a)(1)(B)(i), (a)(2)(A), and (h). Specifically:

a. to the extent that the Defendant Property was derived from a wire fraud offense committed in violation of 18 U.S.C. § 1343 and/or from a violation of IEEPA, 50 U.S.C. § 1705, and was involved in a financial transaction conducted with the intent to commit a violation, or an additional violation, of IEEPA, the Defendant Property was involved in a violation of 18 U.S.C. § 1956(a)(1)(A)(i) and/or a conspiracy to violate that statute;

b. to the extent that the Defendant Property was derived from a wire fraud offense committed in violation of 18 U.S.C. § 1343 and/or from a violation of the IEEPA, 50 U.S.C. § 1705, and was involved in a financial transaction conducted for the purpose of concealing and disguising the source, nature, location, ownership and control of such property, the property was involved in a violation of 18 U.S.C. § 1956(a)(1)(B)(i), and/or a conspiracy to violate that statute; and

c. to the extent that the Defendant Property was involved in a conspiracy to send property from the United States or through the United States to a foreign country with the intent to commit a violation of IEEPA, the Defendant Property was involved in a conspiracy to violate the international promotional money laundering statute, 18 U.S.C. § 1956(a)(2)(A).

8. The Defendant Property is also subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C) because it is the proceeds of a violation of the wire fraud statute, 18 U.S.C. § 1343, and of IEEPA, 50 U.S.C. § 1705.

BACKGROUND REGARDING IEEPA

9. The International Emergency Economic Powers Act (IEEPA), 50 U.S.C. § 1701, *et seq.*, granted the President the authority to deal with unusual and extraordinary foreign

threats to the national security, foreign policy, or economy of the United States. Under IEEPA, the President can declare a national emergency and issue Executive Orders that have the full force and effect of law. Among other things, IEEPA empowers the President to impose economic sanctions on a foreign country. It is a crime to willfully violate, attempt to violate, conspire to violate, or cause a violation of any order, license, regulation, or prohibition issued pursuant to IEEPA. 50 U.S.C. § 1705(a).

10. Using the powers conferred by IEEPA, the President and the Executive Branch have issued orders and regulations governing and prohibiting certain transactions with countries, individuals, and entities suspected of proliferating weapons of mass destruction (WMD). On November 14, 1994, the President issued Executive Order (EO) 12938, finding "that the proliferation of nuclear, biological, and chemical weapons ('weapons of mass destruction') and of the means of delivering such weapons, constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States, and [declaring] a national emergency to deal with that threat."

11. On June 28, 2005, the President, to take additional steps with respect to the national emergency described and declared in EO 12938, issued EO 13382 ("Blocking Property of Weapons of Mass Destruction Proliferators and Their Supporters") to target proliferators of WMD and their support networks and to deny designated proliferators access to the U.S. financial and commercial systems. EO 13382 authorized the U.S. Secretary of the Treasury, in consultation with the Secretary of State, "to take such actions, including the promulgation of rules and regulations, as may be necessary to carry out the purposes" of the EO. Pursuant to that authority, on April 13, 2009, the Secretary of the Treasury promulgated the "Weapons of Mass Destruction Proliferators Sanctions Regulations." *See* 31 C.F.R. § 544.101, *et seq*. EO 13382 and the Weapons of Mass

Destruction Proliferators Sanctions Regulations prohibit transactions or dealings by any U.S. person or within the United States with individuals and entities designated under these authorities, and they further prohibit any transactions that evade or avoid, or have the purpose of evading or avoiding, any prohibitions set forth in the regulations.

BACKGROUND REGARDING THE NORTH KOREA SANCTIONS PROGRAM

12. Beginning with Executive Order No. 13466, issued pursuant to IEEPA on June 26, 2008, the President found that the situation "on the Korean Peninsula constitute[s] an unusual and extraordinary threat to the national security and foreign policy of the United States and . . . declare[d] a national emergency to deal with that threat."

13. On March 15, 2016, to take additional steps with respect to the national emergency described in EO 13466 and to address North Korea's continuing pursuit of its nuclear and missile programs, the President issued Executive Order No. 13722, which prohibits both "the exportation or reexportation, direct or indirect, from the United States, or by a United States person, wherever located, of any goods, services, or technology to North Korea" and "any approval, financing, facilitation, or guarantee by a United States person, wherever located, of a transaction by a foreign person where the transaction by that foreign person would be prohibited by this section if performed by a United States person or within the United States." EO 13722 further prohibits any transactions that evade or avoid, or have the purpose of evading or avoiding, any prohibitions set forth in those regulations.

14. To implement these Executive Orders and others concerning North Korea, OFAC issued the "North Korea Sanctions Regulations." *See* 31 C.F.R. § 510.101, *et seq*. OFAC amended and reissued the regulations in their entirety on March 5, 2018.

15. According to the U.S. Department of the Treasury, the global financial system, trade flows, and economic development rely on correspondent banking relationships. To protect this system from abuse, U.S. financial institutions must comply with anti-money laundering and countering the financing of terrorism requirements set forth in the Bank Secrecy Act (BSA), as well as sanctions and blocking programs administered by OFAC. The Treasury Department's Financial Crimes Enforcement Network (FinCEN) is responsible for administering the BSA in furtherance of its mission to safeguard the U.S. financial system.

16. Section 311 of the USA PATRIOT Act, codified at 31 U.S.C. § 5318A, as part of the BSA, gives FinCEN a range of options, called special measures, that can be adapted to target specific money laundering and terrorist financing concerns.

17. A Section 311 finding and the related special measure are implemented through various orders and regulations incorporated into 31 C.F.R. Chapter X. A violation of 31 U.S.C. § 5318A is punishable criminally pursuant to 31 U.S.C. § 5322.

18. In order to protect the integrity of the U.S. financial system, a Section 311 finding can legally prevent U.S. financial institutions from engaging in any type of financial transaction with an entity within the jurisdiction deemed an area of money-laundering concern.

19. In May 2016, FinCEN made a Section 311 finding against North Korea. Specifically, FinCEN's finding deemed the entire North Korean economy as a primary jurisdiction of money-laundering concern. *See* Federal Register, Vol. 81, No. 107 (June 3, 2016). To make such a finding, FinCEN was able to draw upon administrative subpoenas, prior law enforcement investigations, and voluminous BSA data.

20. In November 2016, FinCEN implemented the most severe special measure against the entire North Korean economy. *See* Federal Register, Vol. 81, No. 217 (November 9, 2016).

The special measure bars domestic and foreign financial institutions from maintaining U.S. correspondent accounts for any North Korean financial institution or party acting on its behalf. Because of the finding that the entire North Korean financial sector was a primary money laundering concern, FinCEN cut all North Korean entities off from any trade in U.S. dollar transactions via correspondent banking. One expert described the effect of such action was to cut the target off from trade in dollars, thereby isolating it from worldwide business.

21. FinCEN targeted the entire North Korean economy because it is comprised entirely of state-controlled financial institutions that use "front companies to conduct international financial transactions that support the proliferation of weapons of mass destruction [] and the development of ballistic missiles in violation of international and U.S. sanctions," and because North Korean financial institutions are subject to "little or no bank supervision or anti-money laundering or combating the financing of terrorism [] controls." *See* Federal Register, Vol. 81, No. 217 at 78715.

22. As detailed further below, FinCEN's Section 311 action included a finding that North Korean financial institutions continued to access the U.S. financial system, in violation of the U.S. sanctions. The finding further stated that millions of U.S. dollars' worth of illicit transactions flowed through U.S. correspondent accounts in spite of the sanctions because of the coordinated use of money laundering techniques to conceal North Korea's involvement and the processing of the payments by North Korean financial institutions. Federal Register, Vol. 81, No. 107 at 35442.

BACKGROUND REGARDING NORTH KOREA'S FOREIGN TRADE BANK

23. On March 11, 2013, the Department of the Treasury designated North Korea's Foreign Trade Bank (FTB), North Korea's primary foreign exchange bank, pursuant to EO 13382,

for providing financial services that assisted in the proliferating of WMD. In the designation, the Treasury Department stated, "North Korea uses FTB to facilitate transactions on behalf of actors linked to its proliferation network, which is under increasing pressure from recent international sanctions. . . . By designating FTB, the Treasury Department is targeting a key financial node in North Korea's WMD apparatus and cutting it off from the U.S. financial system. FTB is a state-owned bank established in 1959. FTB acts as North Korea's primary foreign exchange bank and has provided key financial support to [another designated entity, Korea Kwangson Banking Corp.]." As a result of the designation, FTB was added to Treasury's Specially Designated National ("SDN") List, which is published on its website.

BACKGROUND REGARDING NORTH KOREAN IT WORKERS

24. According to the August 28, 2020 and March 4, 2021 reports by the United Nations Security Council Panel of Experts, one of the ways North Korea generates illicit revenue is by exploiting online platforms that provide opportunities for freelance and contract work, usually in the information technology ("IT") industry. In other words, North Koreans apply for jobs in remote IT development work, including in the virtual currency industry, without disclosing that they are North Korean. These IT workers bypass security and due diligence checks to acquire accounts on these platforms. Specifically, they (1) use obfuscation strategies to create and maintain accounts, such as virtual private networks, to hide their true location from online payment facilitators and hiring platforms, and (2) use fraudulent, or fraudulently obtained, identity documents to obfuscate their true identity and circumvent know your customer (or "KYC") controls.

25. According to a separate report published by a Washington, D.C.-based nonprofit, which conducts analysis of global conflict and transnational security issues, 80% of North Korea's overseas labor force is reportedly stationed in China and Russia. Other countries reportedly hosting

North Korean overseas laborers include, among others, the United Arab Emirates (UAE) and Angola.

26. These IT workers commonly utilize various payment processing services and financial services platforms, including virtual currency exchanges (or VCEs). Many of these services platforms used by IT workers are headquartered in the U.S. Because North Korea is heavily sanctioned and excluded from the U.S. financial system, IT workers circumvent KYC controls that are put in place to ensure said services and platforms do not violate U.S. sanctions imposed on North Korea. North Koreans have been observed utilizing front companies, fraudulent identity documents, stolen identity documents, and identity documents that may have been purchased for North Korea's use to gain access to otherwise prohibited financial services.

27. The FBI, along with the Department of State and Department of the Treasury, issued a May 2022 advisory[3] to alert the international community, private sector, and general public about the North Korean IT worker threat. The United States and the Republic of Korea (South Korea) co-issued updated guidance in October 2023.[4] Then, the FBI supplemented that guidance with additional information in May 2024.[5] The updated guidance includes indicators to watch for that are consistent with North Korean IT worker fraud schemes.

BACKGROUND REGARDING VIRTUAL CURRENCY

28. **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

[3] https://ofac.treasury.gov/media/923126/download?inline

[4] https://www.ic3.gov/PSA/2023/PSA231018

[5] https://www.ic3.gov/PSA/2024/PSA240516

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.

29. **Blockchain:** A blockchain is a digital ledger run by a decentralized network of computers referred to as "nodes." Each node runs software that maintains an immutable and historical record of every transaction utilizing that blockchain's technology. Many digital assets, including virtual currencies, publicly record all of their transactions on a blockchain, including all of the known balances for each virtual currency address on the blockchain. Blockchains consist of blocks of cryptographically signed transactions, and blocks are added to the previous block after validation and after undergoing a consensus decision to expose and resist tampering or manipulation of the data. There are many different blockchains used by many different virtual currencies. For example, Bitcoin in its native state exists of the Bitcoin blockchain, while Ether (or "ETH") exists in its native state on the Ethereum network.

30. **Blockchain Analysis**: Law enforcement can trace transactions on blockchains to determine which virtual currency addresses are sending and receiving particular virtual currency. This analysis can be invaluable to criminal investigations for many reasons, including that it may enable law enforcement to uncover transactions involving illicit funds and to identify the person(s) behind those transactions. To conduct blockchain analysis, law enforcement officers use reputable, free open-source blockchain explorers, as well as commercial tools and services. These commercial tools are offered by different blockchain-analysis companies. Through numerous unrelated investigations, law enforcement has found the information associated with these tools to

be reliable. In this case, law enforcement used blockchain tracing to uncover the connections between the Defendant Property and this North Korean IT worker conspiracy.

31. **Blockchain Explorer**: A blockchain explorer, also called a block explorer, is software that operates as a blockchain search engine for users to search and review transactional data for any addresses on a particular blockchain. A blockchain explorer uses an application programming interface and blockchain nodes to draw data from a blockchain and uses a database to arrange, visualize, and present the data to a user in a searchable format. This data can include average transaction fees, hash rates, and block size.

32. **Decentralized Finance**: Decentralized Finance, or DeFi, is an umbrella term for peer-to-peer financial services on public blockchains, primarily the Ethereum network, that do not require traditional centralized financial intermediaries. DeFi platforms can offer a range of financial services involving digital assets, including the ability for users to lend, invest, earn interest, and exchange digital assets. DeFi platforms provide these services by using self-executing agreements written in code, known as "smart contracts," and these smart contracts are made accessible to users through decentralized applications (or "DApps").

33. **Key Pair**: A key pair, in cryptography, refers to a private key and its corresponding public key. A key pair is used with a public-key algorithm.

34. **Peel Chains**: A peel chain is a technique used to launder a large amount of virtual currency through a lengthy series of minor transactions. It occurs when virtual currency sitting at one address is sent through a series of transactions in which a slightly smaller amount of virtual currency is transferred to a new address each time. In each transaction, some quantity of virtual currency "peels off" the chain to another address (frequently, to be deposited into a VCE), and the remaining balance is transferred to the next address in the peel chain.

35. **Private Key**: A private key is a cryptographic key that is uniquely associated with an entity and not made public. In the blockchain and virtual currency context, virtual currency addresses are controlled using a unique corresponding private key, the equivalent of a password, which is needed to access the funds associated with the address. Only the holder of an address's private key can authorize a transfer of virtual currency from that address to another address.

36. **Public Key**: A public key is a cryptographic key that is uniquely associated with a person or entity and is designed to be made public. The public key is paired with, and derived from, a private (secret) key. However, knowing the public key does not reveal any information about the private key. In the blockchain and virtual currency context, a virtual currency address is the hashed value of a public key and acts as an identifier on a blockchain.

37. **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 and USDT are stablecoins 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.

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

39. **Circle:** Circle Internet Financial, LLC ("Circle") is a U.S.-based VCE that manages the smart contracts and the treasury for USDC tokens.

40. **Transaction Fee**: A transaction fee is a fee paid by the party sending virtual currency on a blockchain to reward miners and/or validators for verifying and validating transactions. Transaction fees vary by blockchain and can fluctuate based on factors such as blockchain network traffic and transaction sizes. Senders of virtual currency can increase the

transaction fees that they pay to have their transactions confirmed faster by miners and/or validators. Transaction fees are generally paid in a blockchain's native token (e.g., Bitcoin on the Bitcoin blockchain). On the Ethereum network, these transaction fees are called "gas fees." Gas fees are transaction costs paid in ETH, or its fraction, gwei. These fees serve as a form of remuneration for validators who maintain and secure the network. Gas fees fluctuate based on supply, demand, and network capacity, and may increase during periods of network congestion.

41. **Transaction Hash**: A transaction hash, also called a transaction ID, is a unique string of characters which identifies a specific transaction on the blockchain—akin to a serial number or accounting journal entry number. A transaction hash is assigned to a transaction when it is added to the blockchain, and it is generated by applying a hash function to the transaction details, including the sender's address, the receiver's address, and the amount of virtual currency being sent. Transaction hashes can be found on blockchain explorers and can be used to verify and track transactions.

42. **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 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.

43. **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.

44. **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).

45. **Virtual Currency Wallet**: A virtual currency wallet (e.g., a hardware wallet, software wallet, or paper wallet) stores a user's public and private keys, allowing a user to send and receive virtual currency stored on the blockchain. Multiple virtual currency addresses can be controlled by one wallet.

46. **Hosted Wallet**: A hosted wallet, also known as a custodial wallet, is a virtual currency wallet through which a third party, e.g., a VCE, holds a user's private keys. The third party maintains the hosted wallet on its platform akin to how a bank maintains a bank account for a customer, allowing the customer to authorize virtual currency transactions involving the hosted wallet only by logging into/engaging with the third party's platform.

47. **Unhosted Wallet**: An unhosted wallet, also known as a self-hosted or non-custodial wallet, is a virtual currency wallet through which the user has complete control over storing and securing their private keys and virtual currency. Unhosted wallets do not require a third party's involvement (e.g., a VCE) to facilitate a transaction involving the wallet. An "unhosted virtual currency address" is a virtual currency address associated with an unhosted wallet.

FACTS

A. Overview of the Investigation

48. The FBI has been investigating, and continues to investigate, North Korea's use of illegally obtained virtual currency as a means of producing income for North Korea. This illegally obtained virtual currency is generated, in part, through remote work done by North Korean IT workers deployed around the globe. As detailed below, law enforcement has, among other things, examined voluminous evidence and conducted blockchain trancing in order to identify multiple North Korean IT workers involved in a money laundering conspiracy to support the North Korean government. Those IT workers have generated revenue for North Korea via their jobs at blockchain development (or other virtual currency-centric) companies. To effectuate the scheme, these North Korean IT workers used fraudulent (or fraudulently obtained) identification documents to obtain work and to access financial services through unwitting employers. These unwitting employers often pay the North Korean IT workers in stablecoins, such as USDC and USDT. When those unwitting employers are companies based in the U.S., those companies have unwittingly hired the North Korean IT workers—and paid them their salaries—in violation of U.S. sanctions.

49. In order to send their illegally obtained virtual currency back to North Korea, North Korean IT workers (and/or their money laundering co-conspirators) transfer the virtual currency through a series of transactions designed to hide the source from which the funds came. For

example, North Korean IT workers (and/or their money laundering co-conspirators) have used the following money laundering techniques: (1) setting up accounts with fictitious identities; (2) moving funds in a series of small amounts; (3) moving funds to other blockchains or converting funds to other forms of virtual currency (i.e., "chain hopping" and "token swapping," respectively); (4) purchasing NFTs as a store of value and means of hiding illicit funds; (5) using U.S.-based online accounts to legitimize activity; and (6) commingling their fraud proceeds to hide the origin of the funds.

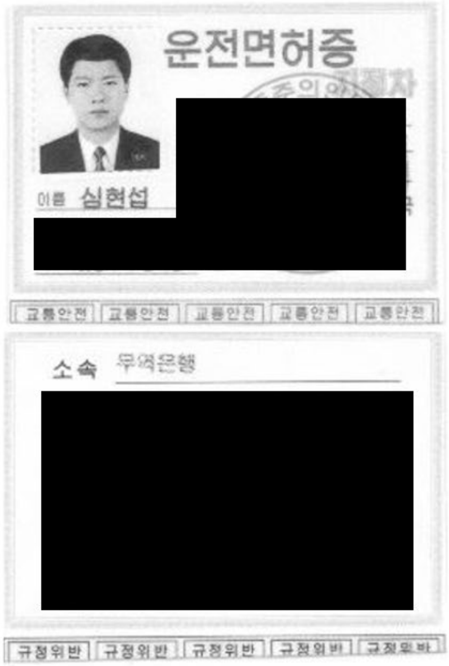
50. After laundering these funds, the North Korean IT workers send them back to the North Korean government, at times via Sim Hyon Sop ("SIM") and Kim Sang Man ("KIM"). As explained below, SIM is a North Korean official employed by North Korea's Foreign Trade Bank (FTB). KIM is a North Korean national who is the chief executive officer (CEO) of "Chinyong," also known as "Jinyong IT Cooperation Company." Chinyong is subordinate to North Korea's Ministry of Defense (formerly known as the Ministry of the Peoples' Armed Forces), which OFAC added to its SDN list on June 1, 2017. Chinyong employs delegations of North Korean IT workers that operate in, among other countries, Russia and Laos. KIM acts as an intermediary between the North Korean IT workers and North Korea's FTB by sending funds from the North Korean IT workers to SIM.

51. On April 24, 2023, OFAC added SIM to its SDN list. On May 23, 2023, OFAC added Chinyong and KIM to its SDN list.

52. The Defendant Property are made up of funds generated by North Korean IT workers—some of whom were unwittingly employed by U.S.-based companies—and sent to KIM and/or SIM for the benefit of the North Korean government.

B. Background Regarding SIM and KIM

53. SIM Hyon Sop (SIM) is a North Korean national and FTB representative. At times, SIM worked for the FTB while living in Dubai, UAE. Within search warrant returns for an email account utilized by SIM ("SIM's Email Account 1"), law enforcement discovered SIM's UAE residency card. Law enforcement also found SIM's North Korean driver's license, which indicates that he is employed by FTB. SIM's UAE residency card and North Korean driver's license are depicted below:



운전면허증

이름 심현섭

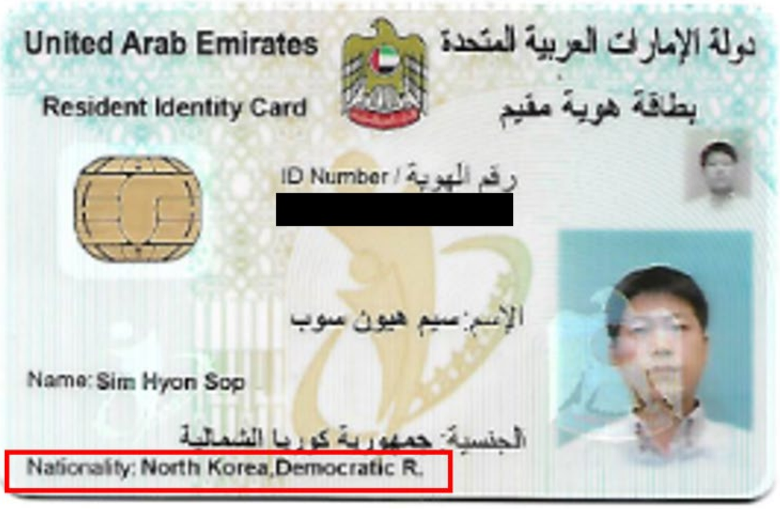
[redacted]

교통안전 교통안전 교통안전 교통안전 교통안전

소속 무역은행

[redacted]

규정위반 규정위반 규정위반 규정위반 규정위반



United Arab Emirates

دولة الإمارات العربية المتحدة

Resident Identity Card

بطاقة هوية مقيم

ID Number / رقم الهوية

[redacted]

الإسم: سيم هيون سوب

Name: Sim Hyon Sop

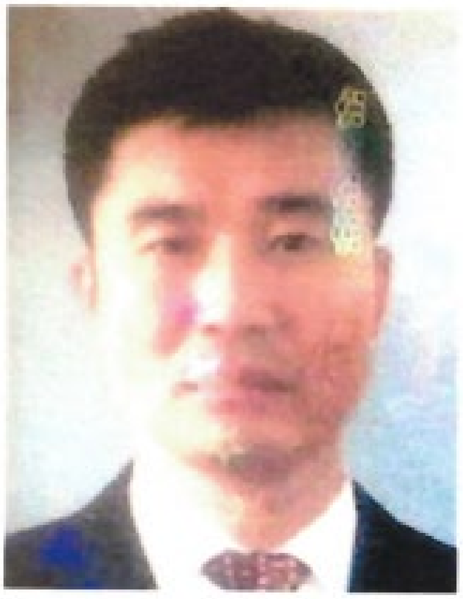
الجنسية: جمهورية كوريا الشمالية

Nationality: North Korea,Democratic R.

54. A review of search warrant returns for SIM's Email Account 1 and of search warrant returns for a second email account utilized by SIM ("SIM's Email Account 2") revealed emails between SIM and his money laundering co-conspirators (including other FTB officials) in which they discuss procurement and banking matters. These emails include information about, among other things, bills of lading, invoices, U.S. dollar loan agreements, fiat currency conversion

agreements, and SWIFT[6] payment confirmations. These emails confirm SIM's role as an FTB representative.

55. KIM is a North Korean national. He is the head of Chinyong and was formerly a representative of Korea Computer Center, a state-run IT research and development center.[7] Chinyong is subordinate to the Korea People's Army (KPA)[8] and is responsible for deploying dozens of North Korean IT workers to Dubai, Laos, Russia, and China. KIM is pictured below:



56. As previously stated, on May 23, 2023, OFAC designated KIM. According to OFAC's press release regarding the designation, KIM was a representative of Chinyong and was

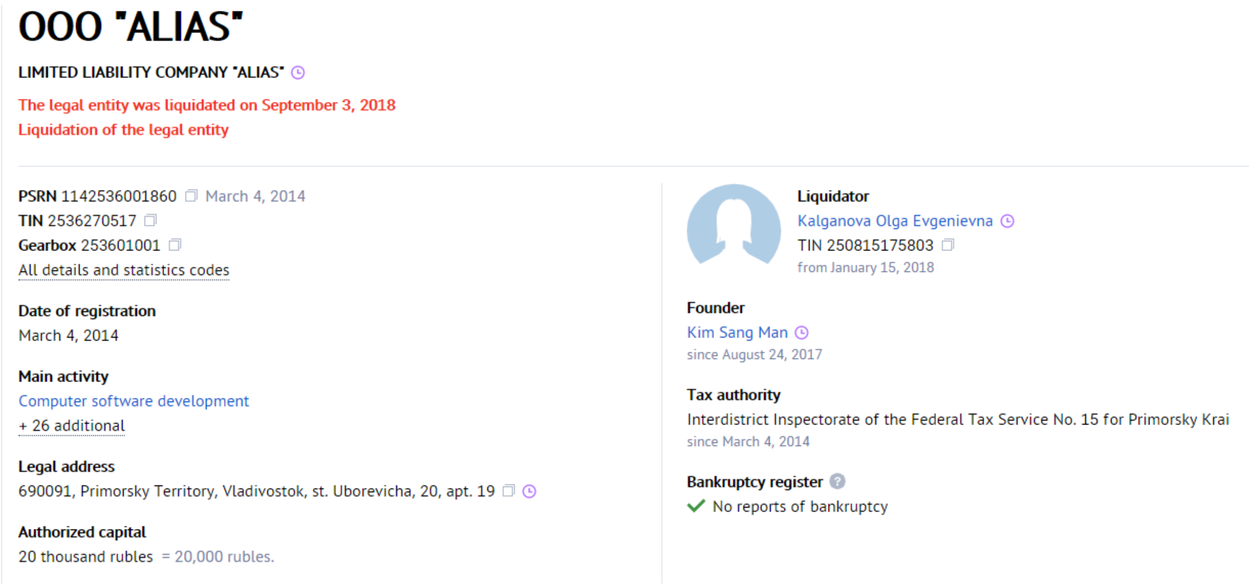
[6] SWIFT stands for Society for Worldwide Interbank Financial Telecommunication. SWIFT payments are payment transactions using the SWIFT international payment network. This network is used to send or receive international electronic payments.

[7] On June 1, 2017, OFAC added Korea Computer Center (KCC) to its SDN list. According to OFAC's press release for the KCC designation, KCC obtained foreign currency for the UN- and U.S.-designated Munitions Industry Department, which is responsible for overseeing North Korea's ballistic missiles.

[8] On June 1, 2017, OFAC added the KPA to its SDN list pursuant to EO 13722. The KPA is the armed forces of North Korea and controlled by North Korea's supreme leader, KIM Jong Un.

designated for engaging in revenue generation for the Workers' Party of Korea (i.e., the ruling party of North Korea), which is also OFAC designated.

57. According to publicly available business records from the Russian Federation, KIM established at least two companies in Vladivostok, Russia that are focused on software development. Those companies are Alis LLC and Alias LLC. The company registration records are depicted below:



OOO "ALIAS"

LIMITED LIABILITY COMPANY "ALIAS"

The legal entity was liquidated on September 3, 2018
Liquidation of the legal entity

PSRN 1142536001860 March 4, 2014
TIN 2536270517
Gearbox 253601001
All details and statistics codes

Date of registration
March 4, 2014

Main activity
Computer software development
+ 26 additional

Legal address
690091, Primorsky Territory, Vladivostok, st. Uborevicha, 20, apt. 19

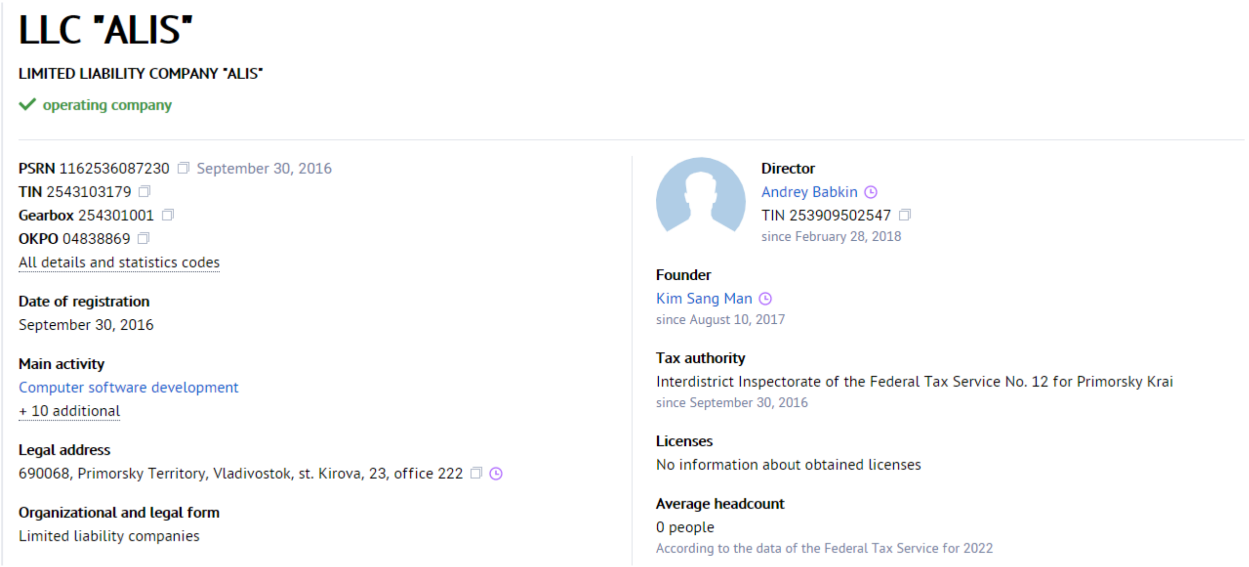
Authorized capital
20 thousand rubles = 20,000 rubles.

Liquidator
Kalganova Olga Evgenievna
TIN 250815175803
from January 15, 2018

Founder
Kim Sang Man
since August 24, 2017

Tax authority
Interdistrict Inspectorate of the Federal Tax Service No. 15 for Primorsky Krai
since March 4, 2014

Bankruptcy register
✓ No reports of bankruptcy



LLC "ALIS"

LIMITED LIABILITY COMPANY "ALIS"

✓ operating company

PSRN 1162536087230 September 30, 2016
TIN 2543103179
Gearbox 254301001
OKPO 04838869
All details and statistics codes

Date of registration
September 30, 2016

Main activity
Computer software development
+ 10 additional

Legal address
690068, Primorsky Territory, Vladivostok, st. Kirova, 23, office 222

Organizational and legal form
Limited liability companies

Director
Andrey Babkin
TIN 253909502547
since February 28, 2018

Founder
Kim Sang Man
since August 10, 2017

Tax authority
Interdistrict Inspectorate of the Federal Tax Service No. 12 for Primorsky Krai
since September 30, 2016

Licenses
No information about obtained licenses

Average headcount
0 people
According to the data of the Federal Tax Service for 2022

58. The FBI's investigation indicates that KIM—at times relevant to the money laundering described herein—was living in Vladivostok, Russia.

C. **Overview Regarding the Movement of Funds from North Korean IT Workers to KIM and SIM**

59. As previously stated, North Korea evades U.S. sanctions by deploying IT workers abroad. Those IT workers target private companies to gain employment and generate substantial revenue for the regime. Once they obtain employment, the North Korean IT workers ask to be paid in stablecoins that they then launder and send to North Korea's FTB via SIM. The North Korean IT workers prefer to be paid in stablecoins because stablecoins retain a consistent value, as opposed to other virtual currencies which fluctuate in price on a daily basis. Those fluctuations mean that the North Koreans could potentially lose the value and benefit of their labor. The North Korean IT workers also prefer stablecoins because they (and/or their money laundering co-conspirators) can more easily trade stablecoins for fiat currency via over-the-counter (OTC) traders (i.e., traders willing to engage in peer-to-peer transfers/swaps of one kind of virtual currency for another or virtual currency for fiat currency, rather than using conventional exchange platforms). Fiat currency is important to the North Koreans because it is more easily leveraged to buy goods for the benefit of North Korea.

60. As is relevant for purposes of this civil forfeiture action, the FBI has learned that this laundering scheme involved moving funds from North Korean "IT Worker Payment Addresses" to "IT Worker Consolidation Addresses." In the context of this filing, IT Worker Payment Addresses are virtual currency addresses to which North Korean IT workers requested payment from their unwitting employees. IT Worker Consolidation Addresses are the virtual currency addresses that the North Koreans (and/or their money laundering co-conspirators) used to commingle IT worker earnings. All references herein to IT Worker Payment Addresses and IT

Worker Consolidation Addresses in this document are references to unhosted addresses that received funds tied to this North Korean money laundering conspiracy. Additionally, all unhosted addresses referenced herein and in Attachment A are unhosted addresses from which law enforcement seized funds and/or requested a freeze of funds because the funds were involved in and/or proceeds of this money laundering conspiracy. In other words, the unhosted addresses mentioned are some of ***the*** IT Worker Payment Addresses and ***the*** IT Worker Consolidation Addresses defined herein.

61. Eventually, the North Korean IT workers (and/or their money laundering co-conspirators) sent the commingled funds from the IT Worker Payment Addresses and/or the IT Worker Consolidation Addresses to KIM via two Binance accounts (collectively, "KIM's Binance Accounts")[9] and/or to SIM via his virtual currency wallet 0x4F47Bc496083C727c5fbe3CE9CDf2B0f6496270c ("SIM's Wallet"), which was voluntarily frozen by Tether as noted above.[10]

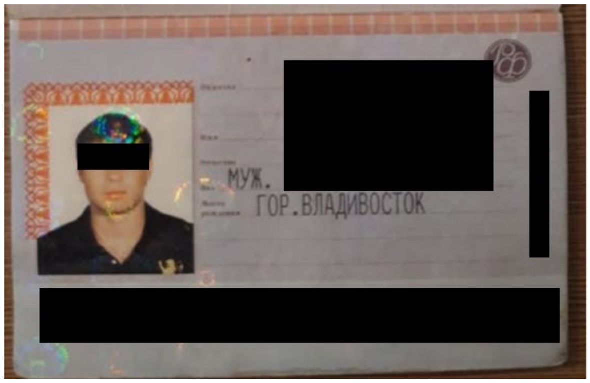
62. Notably, law enforcement's extensive blockchain tracing revealed that SIM's Wallet received nearly $24 million worth of various virtual currencies between August 22, 2021, and March 6, 2023, including 11,097,149 USDT. Further, based on blockchain analysis, as of early-March 2022, the vast majority of the 11,097,149 USDT (approximately 98%) came from KIM's Binance Accounts.

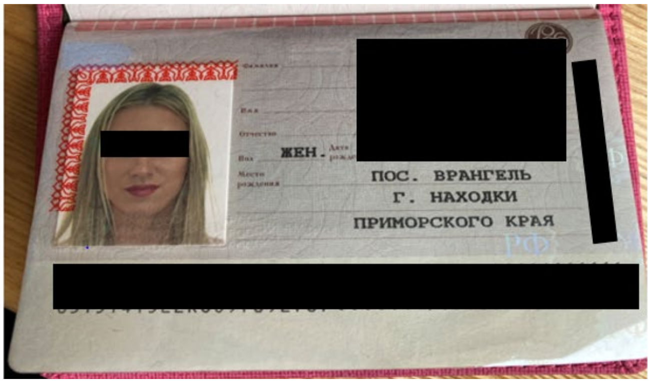
[9] Law enforcement seized KIM's Binance Accounts pursuant to seizure warrant 22-sz-6. As explained above, that property is referred to herein as part of the March 2022 Seized Property.

[10] Tether froze SIM's Wallet on March 6, 2023, meaning that SIM (and his co-conspirators) were no longer able to withdraw USDT from SIM's Wallet after that date.

D. KIM's Binance Accounts Were Registered Using Fraudulent Identity Documents

63. According to records from Binance, a substantial portion of funds sent to SIM's Wallet came from KIM's Binance Accounts. KIM's Binance Accounts were established using two different sets of Russian identity documents, which are depicted below:


[redacted]
[redacted]
МУЖ.
ГОР.ВЛАДИВОСТОК
[redacted]
[redacted]


[redacted]
[redacted]
ЖЕН
ПОС. ВРАНГЕЛЬ
Г. НАХОДКИ
ПРИМОРСКОГО КРАЯ
[redacted]
[redacted]

64. Although KIM's Binance Accounts were established with Russian identity documents, Binance records indicate that (1) both accounts were accessed via the same electronic devices and (2) those electronic devices were set with Korean language preference settings, not Russian.

E. SIM Saved KIM's Phone Number in His Contacts List

65. According to records from Binance, the phone number used to register one of KIM's Binance Accounts was Russia-based phone number +79510124209. Importantly, SIM had that phone number stored in his contacts folder as "Sang Man – Russian Federation." In other words, SIM had KIM Sang Man's phone number in his contacts list.

F. KIM's Binance Accounts Received Funds Tied to North Korean IT Workers

66. KIM's Binance Accounts received funds from multiple IT Worker Payment Addresses and IT Worker Consolidation Addresses. The following are examples of the flow of illicit funds to KIM's Binance Accounts. These examples are not exhaustive. They are simply

meant to provide an overview of how these co-conspirators utilized KIM's Binance Accounts (and North Korean IT workers) to amass virtual currency for the North Korean government.

a. North Korean IT Workers Employed by DeFi Company 1

67. According to blockchain analysis and records from U.S.-based virtual currency exchanges, KIM's Binance Accounts received funds from VCE accounts controlled by U.S.-based companies involved in blockchain and DeFi development. For example, investigation revealed that a U.S.-based IT development company ("DeFi Company 1") sent USDC to two different IT Worker Payment Addresses (collectively, the "Two ITW Addresses"). The Two ITW Addresses then sent funds to KIM's Binance Accounts.

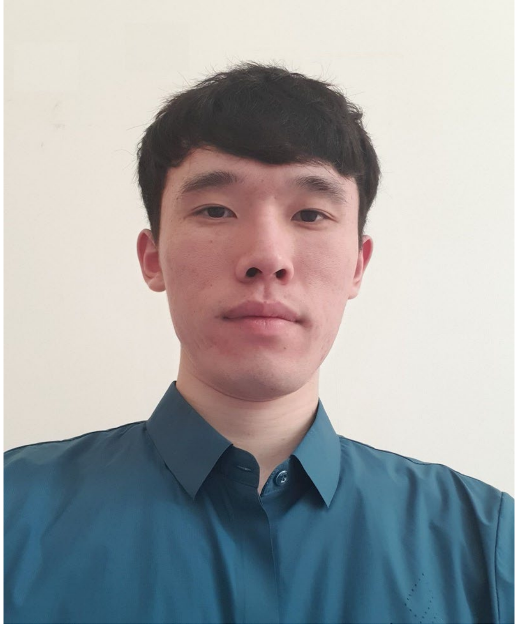
68. Law enforcement interviewed DeFi Company 1's founder and learned that DeFi Company 1 had hired two remote IT workers, who were working as independent contractors, and who asked to be paid via the Two ITW Addresses. DeFi Company 1's founder also indicated to law enforcement that payment to those two employees was sent from DeFi Company 1's corporate account at Coinbase.

69. Law enforcement reviewed DeFi Company 1's employment records related to the two above-referenced IT workers. Law enforcement learned the following about the first IT worker ("IT Worker-1"):

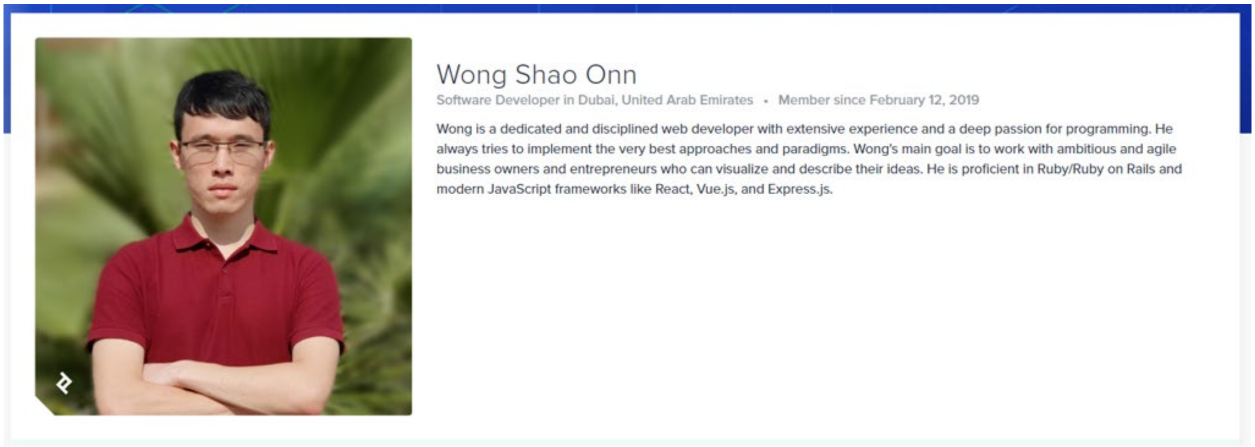
a. IT Worker-1 utilized fraudulent identity information on the W-9 form he submitted to DeFi Company 1. Specifically, the W-9 form indicated that IT Worker-1 was Joshua Palmer ("Palmer"); however, the social security number on the W-9 form belonged to a different U.S. citizen (i.e., that social security number was not tied to Palmer/IT Worker-1), and the physical address on the W-9 form was for a pizzeria, not a residence.

b. IT Worker-1 listed an email account on Palmer/IT Worker-1's resume that was used to establish an account at Binance. That Binance account was registered in the name of Wong Shao Onn ("Onn's Binance Account"), using Malaysian identity documents. Records show that logins for Onn's Binance Account were almost exclusively from UAE-based IP addresses.

c. Additionally, the selfie-style photograph used to create Onn's Binance Account was a picture of Palmer/IT Worker-1 (i.e., the person who worked at DeFi Company 1 and claimed to be Palmer/IT Worker-1). That photograph is depicted below.



d. According to a publicly available posting on a U.S.-based freelance work platform, an individual utilizing the name Wong Shao Onn claimed to be a software developer located in the UAE. A screenshot of that profile page is depicted below.



Wong Shao Onn

Software Developer in Dubai, United Arab Emirates • Member since February 12, 2019

Wong is a dedicated and disciplined web developer with extensive experience and a deep passion for programming. He always tries to implement the very best approaches and paradigms. Wong's main goal is to work with ambitious and agile business owners and entrepreneurs who can visualize and describe their ideas. He is proficient in Ruby/Ruby on Rails and modern JavaScript frameworks like React, Vue.js, and Express.js.

e. The photograph above of Wong Shao Onn appears to be the same person who claimed to be Palmer/IT Worker-1 while working for DeFi Company 1.

f. According to blockchain analysis and records from Binance, the user of Onn's Binance Account sent funds directly to SIM's Wallet and directly to other IT Worker Payment Addresses that then sent funds to KIM's Binance Accounts.

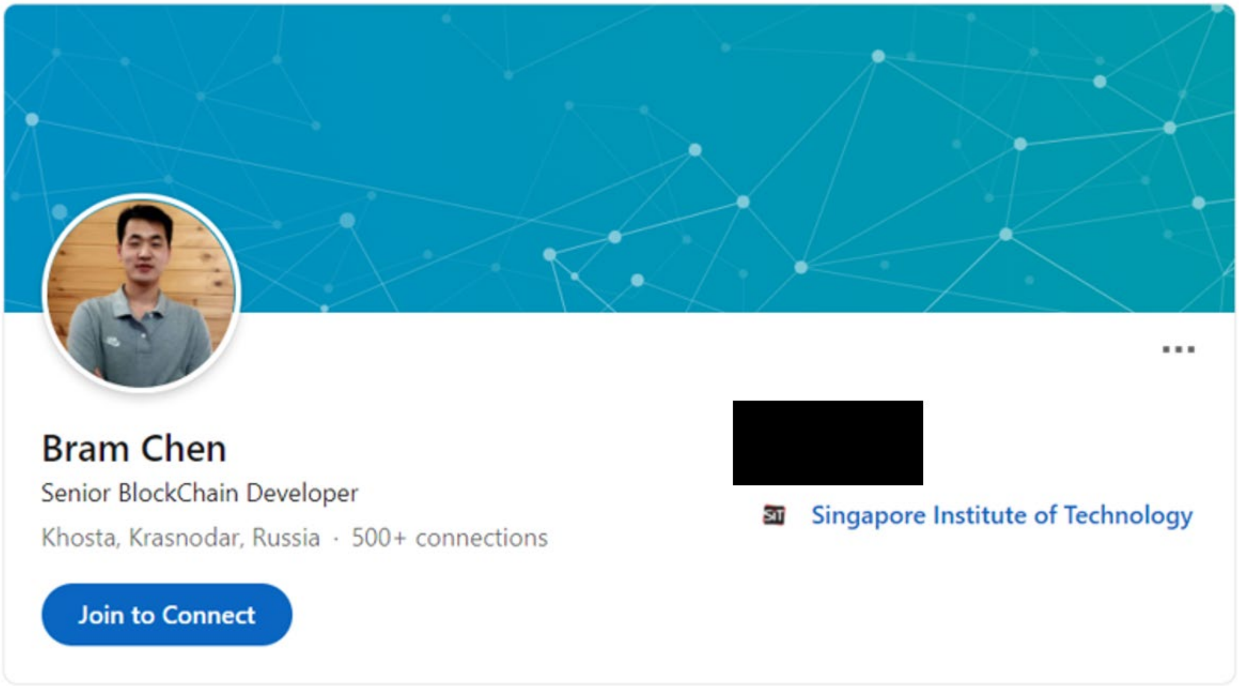
70. Law enforcement learned the following about the second IT worker ("IT Worker-2"):

a. In his application to work for DeFi Company 1, IT Worker-2 claimed to be Bram Chen ("Chen"). Chen was responsible for writing smart contracts.[11] According to Chen's resume, which he supplied to DeFi Company 1, Chen has been employed by several DeFi-centric companies.

b. Chen provided a Russia-based phone number on his resume.

c. Chen's publicly available profile information from a U.S.-based professional networking platform is depicted below:

[11] A smart contract is a type of Ethereum account that can hold funds and can send/refund them based on certain conditions. In DeFi (decentralized finance), a smart contract essentially replaces the financial institution in the transaction.



Bram Chen
Senior BlockChain Developer
Khosta, Krasnodar, Russia · 500+ connections

[redacted]

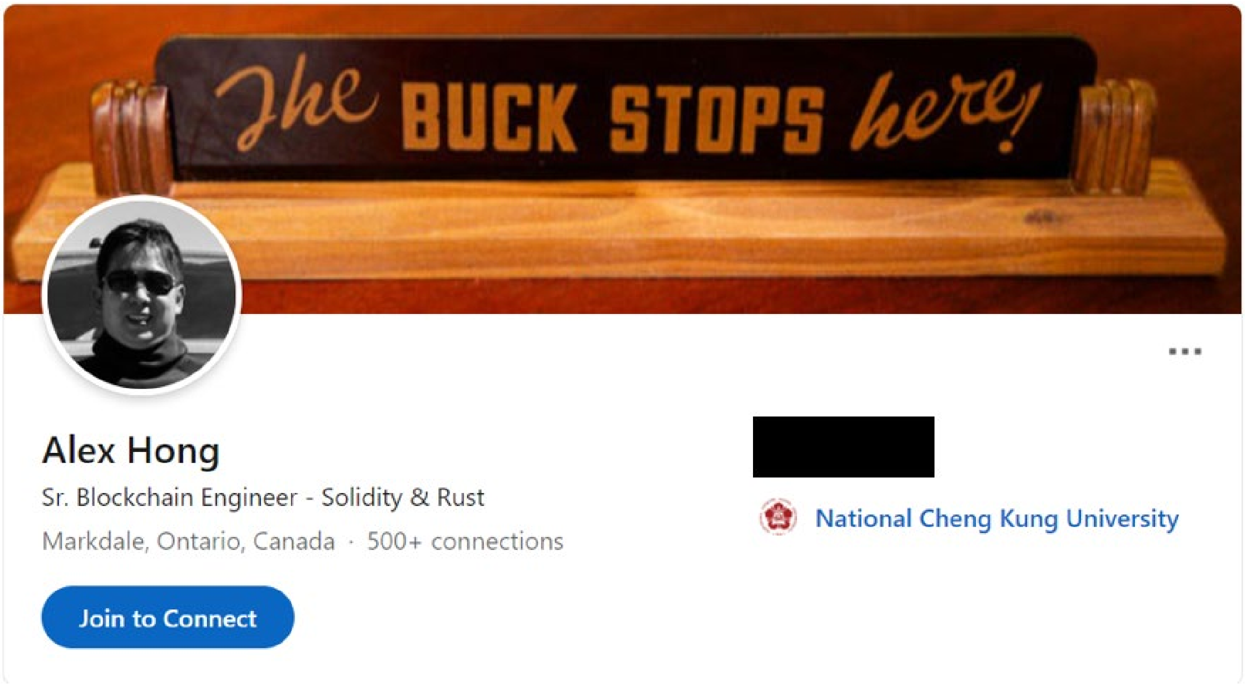
Singapore Institute of Technology

71. On the resume provided by Chen to DeFi Company 1, Chen listed an email account that was also used to register an account with Binance ("Chen's Binance Account"). Based on records from Binance, Chen's Binance Account sent funds directly to one of the IT Worker Consolidation Addresses used to commingle IT worker funds.

b. North Korean IT Workers Employed by DeFi Company 2

72. According to blockchain analysis and records from Binance.US, DeFi Company 2, which is based in the U.S., sent funds to one of the IT Worker Payment Addresses that eventually transferred funds to KIM's Binance Accounts. According to DeFi Company 2's founder, those funds were payment to an individual named Alex Hong ("Hong"), who was hired to create a decentralized application (DApp) for DeFi Company 2. According to DeFi Company 2's founder, Hong initially claimed to be located in Australia. Subsequently, Hong claimed to be in Canada. DeFi Company 2's founder indicated that Hong was also employed by a London-based DeFi

company. Below is a screenshot from a publicly available profile for a user identified as Alex Hong, who claimed to be in Canada and to be employed by the same London-based DeFi company:



Alex Hong

Sr. Blockchain Engineer - Solidity & Rust

Markdale, Ontario, Canada · 500+ connections

[redacted]

National Cheng Kung University

c. IT Workers Use Fraudulent Identity Documents to Establish VCE Accounts

73. While investigating Palmer, Chen, and Hong, law enforcement identified VCE accounts at multiple virtual currency exchanges that (1) were established using fraudulent identification; and (2) were used to launder funds tied to IT Worker Payment Addresses, IT Worker Consolidation Addresses, and KIM's Binance Accounts. For example:

a. The Leech Accounts[12]:

i. According to records provided by Binance, Coinbase, and Bittrex, the same email account was utilized to register accounts at all three

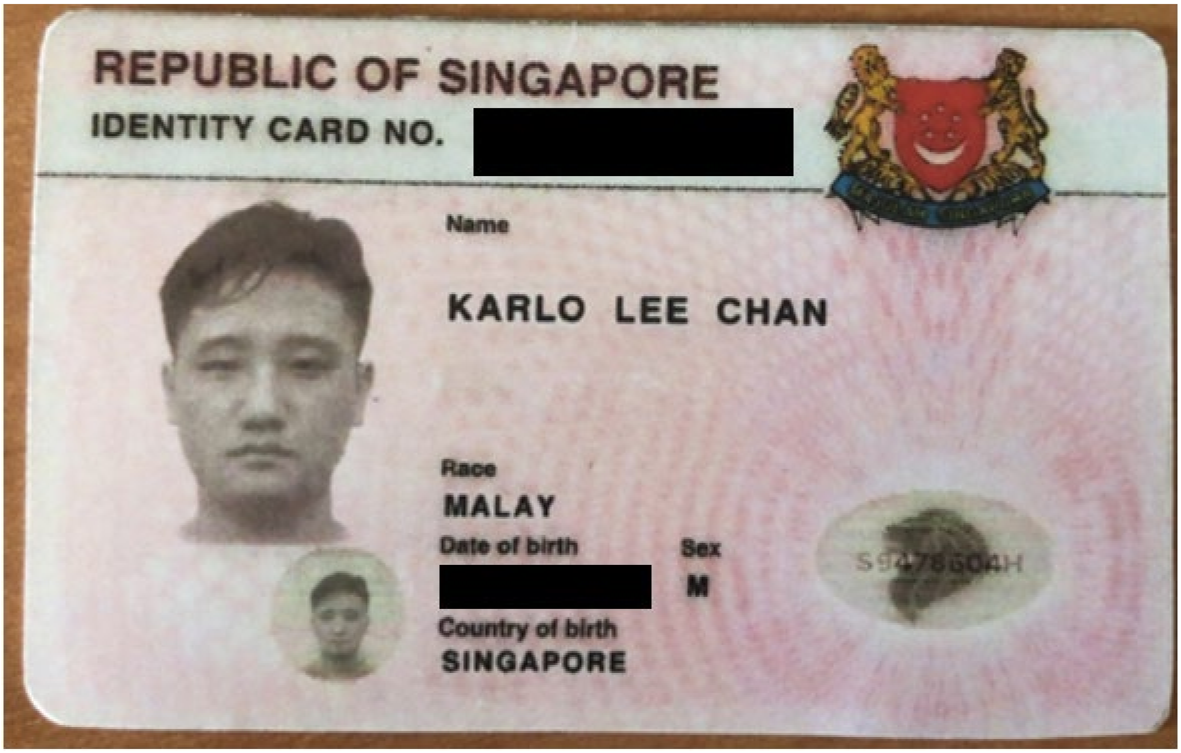
[12] These accounts are referenced herein as the Leech Accounts because the actors associated with the Leech Accounts used names and other identifiers that incorporated the word "leech." For example, as explained below, the actors used the names ***LEE Ch***an and ***LEE Ch***ienhui, as well as the online identifiers "leech_dev" and "leech.developer@gmail.com."

exchanges. Those accounts are referred to herein as the "Binance Leech Account," the "Coinbase Leech Account," and the "Bittrex Leech Account," respectively, and the "Leech Accounts," collectively.

ii. According to records from Binance, the Binance Leech Account was accessed almost exclusively from Russian IP addresses, though nearly all devices accessing the account were set with English language preference.

iii. The Coinbase Leech Account was registered under the name Chienhui Lee, and the user provided a UK-based phone number.

iv. The Bittrex Leech Account was accessed from Russia-based IP addresses but was registered with the Singaporean identity document depicted below, in the name Karlo Lee Chan:



REPUBLIC OF SINGAPORE

IDENTITY CARD NO. [redacted]

Name

KARLO LEE CHAN

Race

MALAY

Date of birth

[redacted]

Sex

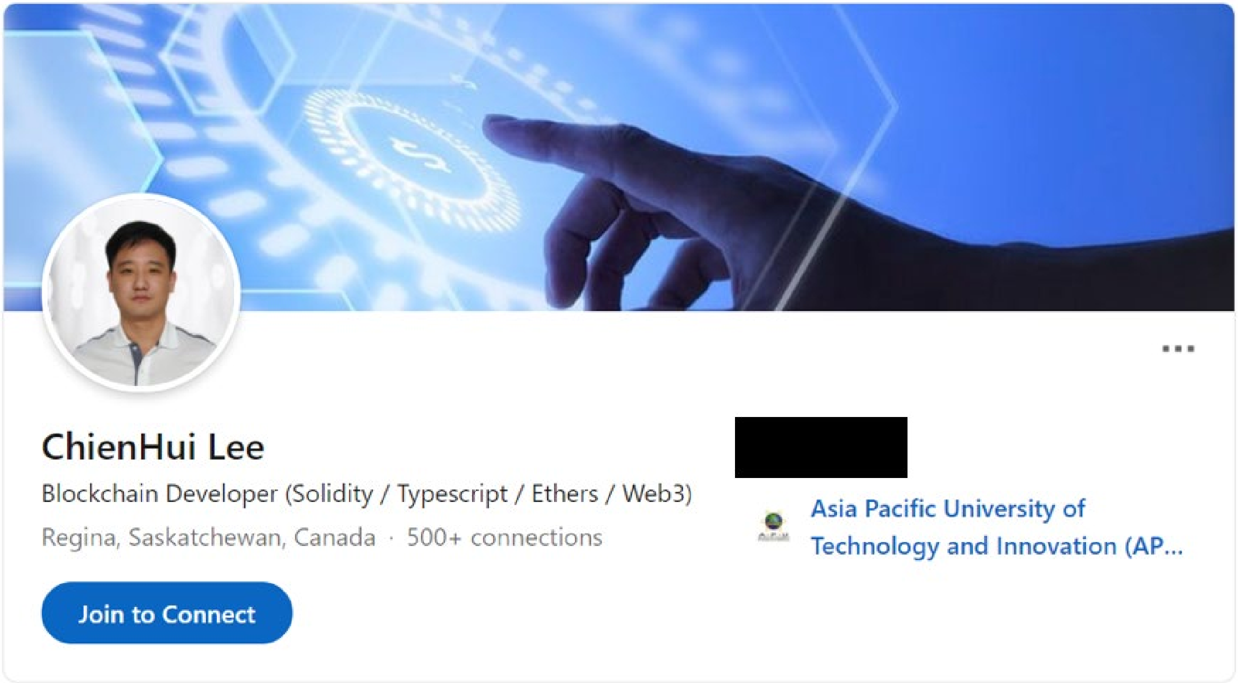
M

Country of birth

SINGAPORE

S9478604H

v. On a site for professional networking and career development, law enforcement identified a profile in the name ChienHui Lee ("Lee"), the same name used to open the Coinbase Leech Account. According to the profile information, Lee was a blockchain developer located in Canada. The networking profile indicated that Lee was employed by a U.S.-based DeFi company. A screenshot of that profile is depicted below:



ChienHui Lee

Blockchain Developer (Solidity / Typescript / Ethers / Web3)

Regina, Saskatchewan, Canada · 500+ connections

[redacted]

Asia Pacific University of Technology and Innovation (AP...

vi. It appears from the Singapore identification card and the networking profile that Karlo Lee Chan and ChienHui Lee are the same person.

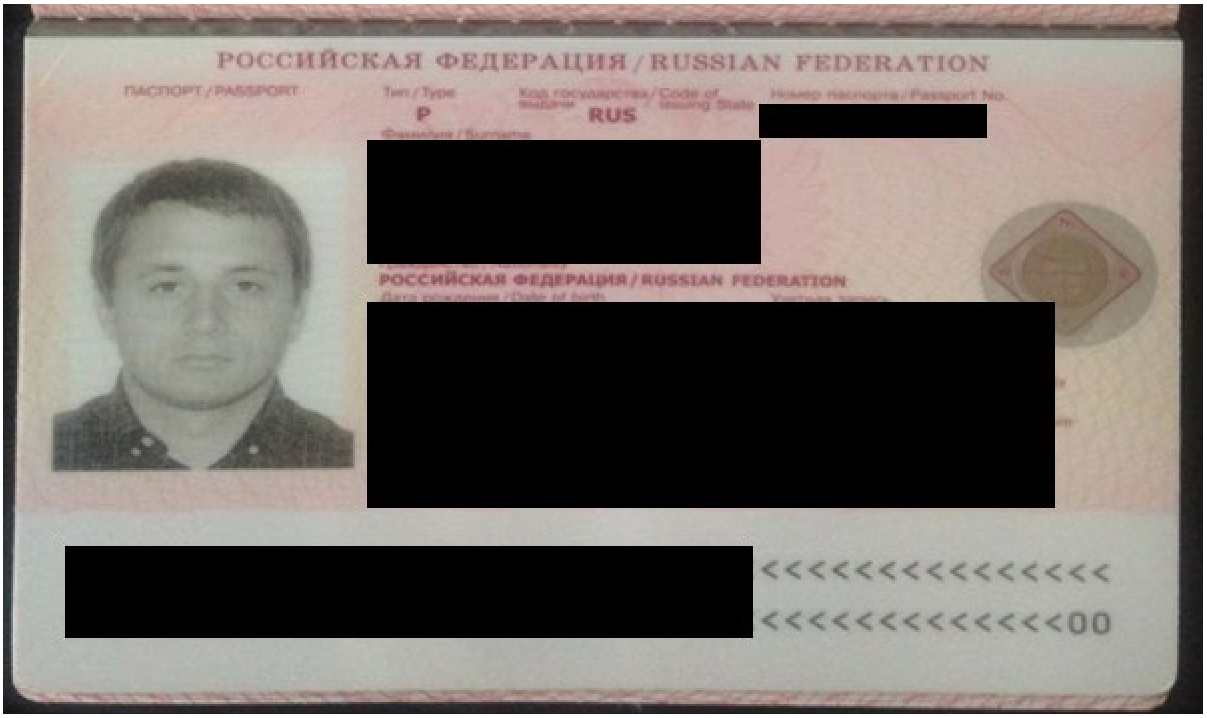
vii. The above indicates that the Leech Accounts are controlled by a person (or people) engaged in fraud. Specifically, the use of the same email, but with different names and geographic locations/IP address connections, indicates to me that the identity information used to open the Leech Accounts is fraudulent.

viii. Additionally, according to blockchain analysis and records from Binance and Bittrex, the Leech Accounts sent funds (including USDT and/or BTC) to IT Worker Payment Addresses and IT Worker Consolidation Addresses before those funds were sent to KIM's Binance Accounts.

ix. As previously stated, North Korean IT workers utilize a variety of means to gain employment and access to financial accounts, including the use of fraudulent identity information. The Leech/Lee persona is consistent with both the type of work sought (i.e., IT development jobs in the virtual currency space) and use of fraudulent information (i.e., false or fraudulently obtained identification information) to gain access to U.S.-based employment and U.S.-based financial services.

b. The Iurii Accounts

i. According to records from Binance, Binance User ID 46842926 was registered under the name Iurii Takhtenkov (the "Binance Iurii Account"). The Binance Iurii Account was established with Russian KYC documents and was primarily accessed from UAE-based IP addresses. The Binance Iurii Account sent funds to IT Worker Consolidation Addresses. Below is a copy of the identification document used to register the Binance Iurii Account:



РОССИЙСКАЯ ФЕДЕРАЦИЯ / RUSSIAN FEDERATION

ПАСПОРТ / PASSPORT

Тип / Type: P

Код государства выдачи / Code of issuing State: RUS

Номер паспорта / Passport No. [redacted]

Фамилия / Surname

[redacted]

РОССИЙСКАЯ ФЕДЕРАЦИЯ / RUSSIAN FEDERATION

Дата рождения / Date of birth

[redacted]

[redacted] <<<<<<<<<<<<<<<

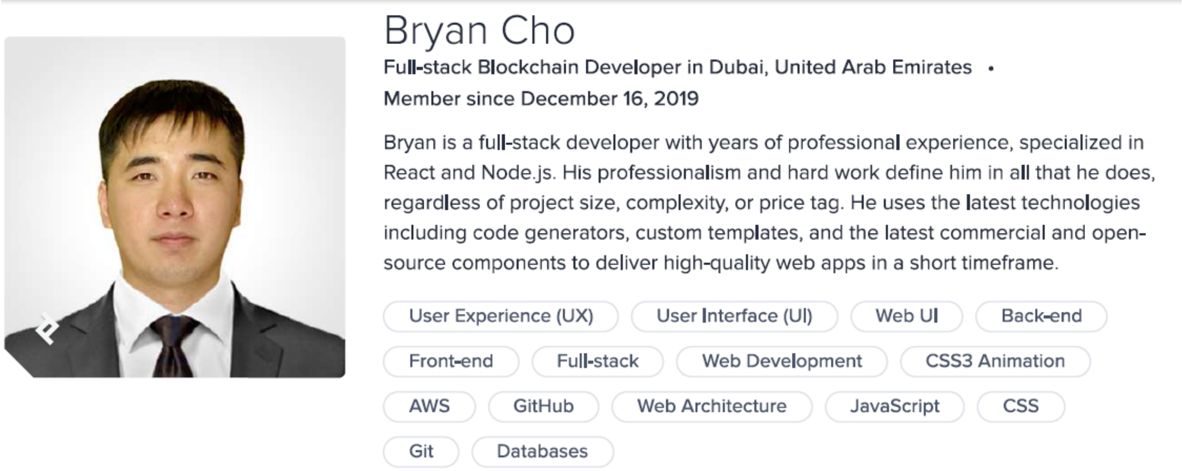
<<<<<<<<<<<<<00

ii. According to records from Bittrex, the same email account used to open the Binance Iurii Account was also used to establish an account at Bittrex (the "Bittrex Iurii Account").

iii. According to records from the internet service provider, the email account used to register both the Binance Iurii Account and the Bittrex Iurii Account was linked by cookie to the email address bryan.cho@toptal.com,[13] indicating that the email accounts were accessed from the same device. According to a publicly available resume in the name of Bryan Cho ("Cho") on Toptal's website, Cho is a UAE-based blockchain developer. Notably, the Cho persona is consistent with both the type of work sought by North Korean IT

[13] Toptal is a company that provides a freelancing platform for connecting businesses with software engineers, designers, finance experts, product managers, and project managers.

workers and the use of fraudulent information to gain access to U.S.-based financial services. A screenshot of Cho's profile is depicted below:



Bryan Cho

Full-stack Blockchain Developer in Dubai, United Arab Emirates •

Member since December 16, 2019

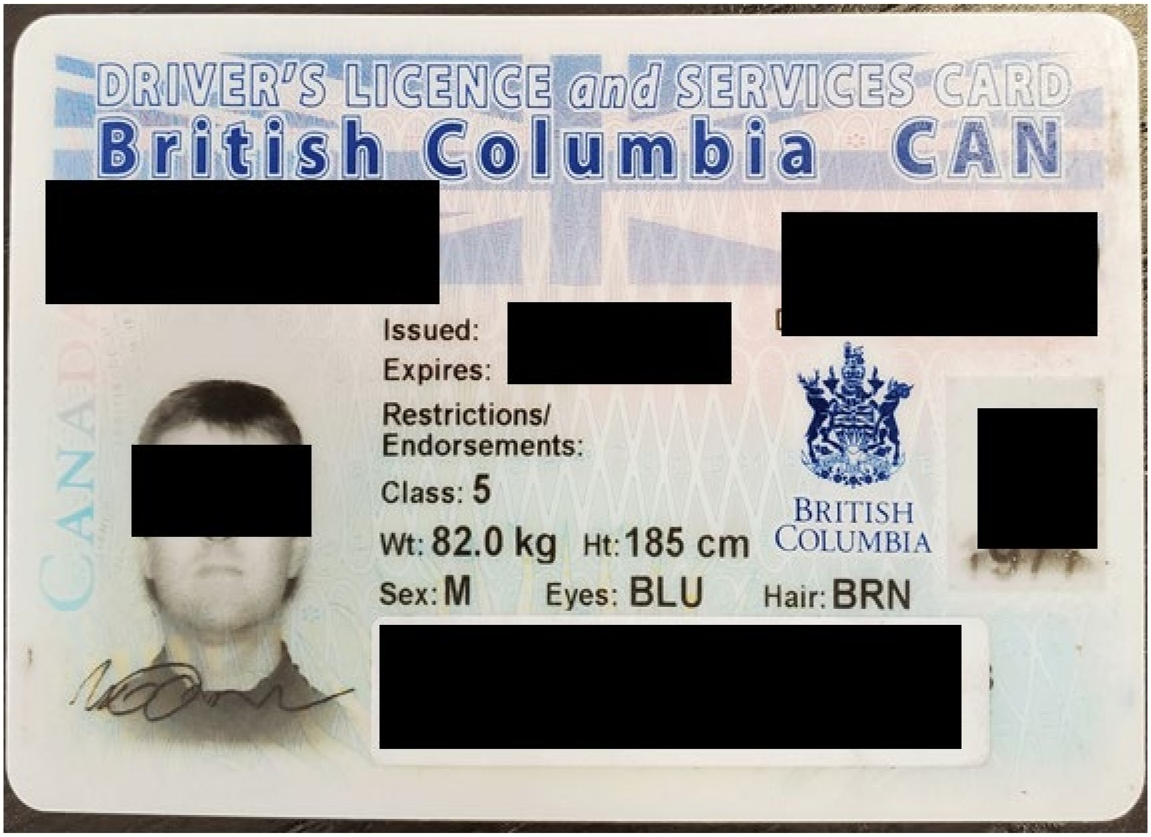
Bryan is a full-stack developer with years of professional experience, specialized in React and Node.js. His professionalism and hard work define him in all that he does, regardless of project size, complexity, or price tag. He uses the latest technologies including code generators, custom templates, and the latest commercial and open-source components to deliver high-quality web apps in a short timeframe.

iv. According to blockchain analysis and records from Binance and Bittrex, the Binance Iurii Account and the Bittrex Iurii Account sent funds (including USDT and BTC) to IT Worker Payment Addresses and IT Worker Consolidation Addresses before those funds were sent to KIM's Binance Accounts.

d. Korean Language Preference for Binance Accounts

74. According to records from Binance, several of the Binance accounts that sent funds to IT Worker Payment Addresses and IT Worker Consolidation Addresses were accessed via devices set with Korean language preference. The language preference for these accounts was inconsistent with the identity document information used to establish the accounts. It was also inconsistent with the geographical location information and IP addresses used to access the accounts. For example, according to records from Binance, User ID 41825291 was established in

the name Mark Anders Liljefors (the "Liljefors Binance Account") with the following Canadian identity document:



DRIVER'S LICENCE and SERVICES CARD

British Columbia CAN

[redacted]

[redacted]

Issued: [redacted]
Expires:

Restrictions/
Endorsements:

Class: 5

Wt: 82.0 kg Ht: 185 cm

Sex: M Eyes: BLU Hair: BRN

BRITISH COLUMBIA

CANADA

[redacted]

[redacted]

[redacted]

75. Although the Liljefors Binance Account was established with a Canadian identity document, the Liljefors Binance Account was predominantly accessed from Russia-based IP addresses. In addition, the majority of the devices used to access the account were set for Korean language preference. The Liljefors Binance Account sent funds to IT Worker Consolidation Addresses, which then sent funds to KIM's Binance Accounts.

76. As previously stated, the above is an overview of this money laundering scheme. During this ongoing investigation, law enforcement encountered many more accounts just like them. In sum, law enforcement learned that these co-conspirators use fraudulent identity documents and layered virtual currency transactions to cloud the source of funds, allowing sanctioned North Korean entities to collect illicit proceeds. These money laundering tactics also

prevent U.S. financial institutions and employers from effectively implementing anti-money laundering controls to prevent violations of U.S. sanctions against North Korea.

CONNECTING THE DEFENDANTS *IN REM* TO THE OVERALL SCHEME

77. As outlined above in paragraphs 2(a) through 2(h), the defendants *in rem* (the Defendant Property) include eight tranches of virtual currency that have either been seized and are in U.S. government wallets or have been frozen by Tether and await transfer to the U.S. government pursuant to this civil forfeiture action. The following paragraphs explain the connections between the eight tranches and the above-described laundering scheme. In sum, law enforcement seized SIM's Wallet, KIM's Binance Accounts, a Binance account believed to be controlled by SIM, and a Binance account that contained funds from IT Worker Payment Addresses. Law enforcement also seized unhosted addresses that are some of the IT Worker Payment Addresses and/or IT Worker Consolidation Addresses that received and contained funds tied to this money laundering conspiracy.

78. Paragraph 2(a):

a. The March 2022 Seized Property (associated with paragraph 2(a) above) includes KIM's Binance Accounts (Binance User ID 81090004 and User ID 118543589) discussed in paragraphs 60 through 74. The March 2022 Seized Property also includes various types of virtual currency that were seized from unhosted virtual currency addresses. Those unhosted addresses are some of the IT Worker Payment Addresses and IT Worker Consolidation Addresses. The March 2022 Seized Property was seized during the execution of seizure warrant 22-sz-6.

79. Paragraph 2(b):

a. The June 2022 Seized Property (associated with paragraph 2(b) above) includes various types of virtual currency that were seized from unhosted virtual currency addresses. Those unhosted addresses are some of the IT Worker Payment Addresses and IT Worker Consolidation Addresses. The June 2022 Seized Property also includes NFTs and ENS domain names that were used to launder proceeds from North Korean IT Workers. The June 2022 Seized Property was seized during the execution of seizure warrant 22-sz-13.

80. Paragraph 2(c):

a. The August 2022 Seized Property (associated with paragraph 2(c) above) includes two Binance accounts, User ID 369902286 and User ID 126474093. The August Seized Property was seized during the execution of seizure warrant 22-sz-18.

b. Regarding Binance User ID 369902286, blockchain analysis revealed that this account was used to send funds to, and receive funds from, SIM's Wallet. Specifically, between December 19, 2021, and September 1, 2022, Binance User ID 369902286 received Binance USD, as well as USDT and USDC on Binance Smart Chain from SIM's Wallet. At the time of those transfers, the funds were valued at approximately $1.45 million. Nearly all funds sent from SIM's Wallet to Binance User ID 369902286 were converted to USDT on the Ethereum blockchain and then sent back to SIM's Wallet. In other words, the funds were sent to Binance User ID 369902286 at Binance so that they could be converted to USDT via Binance's exchange platform, and then almost all of that USDT was sent back to SIM's Wallet. These transactions do not appear to have any utility other than to launder funds.

c. Notably, a review of search warrant returns for an email account used by SIM revealed that he registered his account at a cloud service provider using a phone number ending in 1201. Binance User ID 369902286 was registered at Binance using the same phone number ending in 1201. Additionally, Binance User ID 369902286 was registered with a UAE Resident Identity Card in the name Rifas Kiyasdeen. According to search warrant returns from SIM's email account, SIM used the same identity documents in the name of Rifas Kiyasdeen to register an account with FedEx. In other words, SIM likely controlled Binance User ID 369902286.

d. Regarding Binance User ID 12647409, that Binance account received funds from IT Worker Payment Addresses.

81. Paragraph 2(d) and 2(e):

a. The September 22 Seized Property (associated with paragraph 2(d) above and seizure warrant 22-sz-19), as well as the USDT frozen on or about September 1, 2022 (associated with paragraph 2(e) above) includes USDC and USDT tokens seized from two unhosted virtual currency addresses, 0x815F335f976301f496167bfeF237f0622F92ac38 ("0x815F") and 0x81c4d8816b29147c542dDE87485608204690Acf2 ("0x81c4"). Those unhosted addresses are some of the IT Worker Consolidation Addresses.

b. Those two unhosted virtual currency addresses contained both USDC and USDT tokens. Blockchain analysis revealed that address 0x815F received approximately 12,250 USDC from two of the IT Worker Payment Addresses. Address 0x815F also received approximately 367,550 USDT from IT Worker Consolidation Addresses and 10,000 USDT from one of the IT Worker Payment Addresses. According to blockchain analysis, 0x81c4 received approximately 158,122.85 USDC, on two separate blockchains, from at least ten IT Worker Payment Addresses. 0x81c4 also received approximately 54,574 USDT from at least four IT Worker Payment Addresses.

82. Paragraph 2(f):

a. Paragraph 2(f) relates to USDT that was voluntarily frozen by Tether on or about March 6, 2023, in unhosted virtual currency address 0x4F47Bc496083C727c5fbe3CE9CDf2B0f6496270c (“0x4F47”). Address 0x4F47 is SIM’s Wallet. As described above, SIM’s Wallet received approximately $10 million of USDT from KIM’s Binance Accounts, which were funded in large part by proceeds from the North Korean IT workers who obtained employment from unwitting companies. *See* para. 60, 61, *infra.* SIM’s Wallet also received funds directly from an IT worker’s account. *See* para. 68(f) *infra.*

83. Paragraph 2(g):

a. Paragraph 2(g) relates to USDT that was voluntarily frozen by Tether on or about March 6, 2023, in unhosted virtual currency addresses 0x5707aA6944E357cEa1A25Ff991fB3A2E60268AB5 (“0x5707”) and 0xB389B4B4a8a6E267CA0712321cdca5c856ef8A72 (“0xB389”). Those unhosted addresses are some of the IT Worker Consolidation Addresses.

b. 0x5707 was used to consolidate virtual currency, including USDT from North Korean IT Workers. For example, between June 2022 and March 2023, 0x5707 received approximately 4,577,810 USDT. It also received approximately 192,000 USDT from SIM's Wallet.

c. Finally, 0x5707 sent approximately 3.8 million USDT to addresses associated with a Chinese national named Lu Huaying ("LU"). LU operated as an OTC trader. OFAC added LU to its SDN list on or about December 17, 2024. According to OFAC, LU was designated for working through a UAE-based front company to facilitate money laundering and virtual currency conversion services that funneled illicit proceeds to Pyongyang. The network was led by SIM.

d. When Tether froze 0x5707, it had a balance (and still does) of approximately 200,603 USDT.

e. 0xB389 was used to consolidate virtual currency, including USDT from North Korean IT workers. Between October 2022 and March 2023, 0xB389 received approximately 2,964,101 USDT.

f. In October 2022, 0xB389 sent approximately 43,200 USDT to an account at Binance controlled by SIM.

g. 0xB389 also sent approximately 1.7 million USDT to address 0x511b9ED0b7eF9dfad519f398Fdfbdf6Af8356780 ("OTC 1"). According to records from FTX (a now-defunct VCE), OTC 1 is tied to an FTX account under LU's name. LU opened that FTX account using a UAE residency card.

h. 0xB389 also sent approximately 556,000 USDT to 0x2ad9790b5116ce19b9cc59C7982A64dF0FeA84bc ("OTC 2"). OTC 2 received approximately 12.7 million USDT from SIM's Wallet. OTC 2 received a total of 30,592,211 USDT. Of that amount, OTC 2 sent approximately 21 million USDT to LU's FTX account mentioned above.

i. When Tether froze 0xB389, it had a balance (and still does) of approximately 464,669 USDT.

84. Paragraph 2(h):

a. Paragraph 2(h) relates to USDT voluntarily frozen by Tether on or about April 1, 2023, in unhosted virtual currency addresses 0x15824de78A61a8B493CCd8A48e58463536B17028 ("0x1582"), 0x6E2F0deAB1C358547b353342524489e32640D530 ("0x6E2F"), 0x3E24F610639e105173003EF1c47dC4DbAa33f8D7 ("0x3E24"), and 0x1c097e02bCd6cD69946663ace4bc0B115e256bAc ("0x1c09"). Those unhosted addresses are some of the IT Worker Consolidation Addresses.

b. 0x5707 and 0xB389 (associated with paragraph 2(g)) each received assets from a series of four other IT Worker Consolidation Addresses. After Tether froze addresses 0x5707 and 0xB389, the four IT Worker Consolidation Addresses sent ETH to four new IT Worker Consolidation Addresses, providing the first gas[14] into 0x1582, 0x6E2F, 0x3E24, and 0x1c09. These new IT Worker Consolidation Addresses began receiving virtual currency from dozens of

[14] As explained above, "gas" is a term used to describe the funds required to pay for a transaction on certain blockchains, including the Ethereum network.

unhosted addresses, which were previously sending to 0x5707 and 0xB389. In other words, these co-conspirators began using these four addresses as their new IT Worker Consolidation Addresses for illicit funds.

c. When Tether froze 0x1582, 0x6E2F, 0x3E24, and 0x1c09, they contained approximately 32,163 USDT, 84,814 USDT, 13,300 USDT, and 46,799 USDT, respectively.

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.

May XX, 2025
Washington, D.C.

JEANINE FERRIS PIRRO
Interim United States Attorney

/s/ Rick Blaylock, Jr.
Rick Blaylock, Jr.
Assistant United States Attorney
Asset Forfeiture Coordinator
Texas Bar Number 24103294
United States Attorney's Office
601 D Street NW
Washington, D.C. 20530
Telephone: 202-252-6765

Email: rick.blaylock.jr@usdoj.gov

Jessica C. Peck
New York Bar No. 5188248
Trial Attorney
U.S. Department of Justice, Criminal Division
Computer Crime and Intellectual Property Section
1301 New York Avenue, N.W., Suite 600
Washington, D.C. 20005
(202) 514-1026 (main line)
jessica.peck@usdoj.gov

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
Email: Gregory.Nicosia@usdoj.gov

VERIFICATION

I, Christopher Wong, a Supervisory 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 other 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 23rd day of May 2025.

____
Christopher Wong
Supervisory Special Agent
Federal Bureau of Investigation

ATTACHMENT A

1. Virtual currency seized from unhosted virtual currency addresses and two accounts at Binance (a virtual currency exchange or "VCE") during the execution of seizure warrant 22-sz-6:

Unhosted Address Assets	**Amount**
BTC	0.0088168900
LTC	0.1277800100
ETH	521.8746883372
STARL	29692425251.2506000000
ENS	9356.0348458065
USDT	57108.4877230000
DBUY	3496980.1704557400
KUMA	138831744207.6800000000
USDC	11408.4319970000
CRV	2701.7377850068
DAI	3547.2432407695
SMI	239599819.0021540000
PERP	4.6601186800
GTC	0.0000449293
BNB	1.6022037064
BUSD	6750.0000000000
ABGRT	0.5760000000
MATIC	9.9860082833
FTM	16.8386154779
Binance Account 81090004:	
BNB	0.0000124000
BTC	0.0000073300
ETH	145.7000897500
USDT	1484636.8067804600
SAND	14082.9700000000
USDC	0.7433070000
BUSD	0.4068787400
Binance Account 118543589:	
BNB	0.0000521300
ETH	0.0000350000
USDT	2411417.7593996300

The above-listed assets were seized from the following unhosted addresses. These unhosted addresses are some of the "IT Worker Payment Addresses" and "IT Worker Consolidation Addresses," as defined in the accompanying complaint.

- bc1qrzxvnl8lr4te4hgmz2e0nn97ypq2nyvvev2ges
- LKm8pewKd68MN9Rk6mAeNqSNFovvsLtCz8
- 0x7066D17C140a64e770c7286DeF08C611a9cC78d4
- 0xb41d7De2AF854C17965C277fEb5B55ECc596Ccd8
- 0xb6bb7BE73d453ed6D1141A08E444DaC1356F0766
- 0x0A9Afe0b6E04Fd212aD7547e9798E0A7Ca2EE370
- 0x6c90b98b8C5C41D615300b9ed774F85b29078CA2
- 0xfCe7C3c7717F933895779724851 42e928F231dad
- 0x294662cca316061A5942c7Be3191b96318606781
- 0xd4004F07D7b746103F2D9B4e5B5A540864526BEc
- 0xa7D2cF62487AA87dDba211D1e8DC7259BE2a9A70
- 0x5A297599c4bD1c3ef00b277f8a7369cb5b9Bd157
- 0xA6Ee3542b6ab3115Be7E6445268161E0293ed7cF
- 0xFe035df35C6fE5578EdE6267883638DB7634DE82
- 0x95d179FB2f017FaadD0013F730d949ac0aC739B6
- 0x50e7f5d0f2bA91E002c7094d844D3A8fF187e204
- 0x1690c80F392a8ba83E2f755b1E53Dd4503738698
- 0x6A643519520b875BD9CE7E882c218A6E38d8Dc41
- 0x3269C4C05356E511BC447DA5C722e63f682243C9
- 0x67624c4C72B8989143510f9Ac09A58007bf79676
- 0xdd344126c52478E8e1e7aad583E2332567Afd730
- 0x53C64EC686F8235954d1dF08cD975C337A8f24B2
- 0xa09a934BA4440CFCbD0C2937a263351926919565
- 0xf3F2e9391b440526D538E904C0252421eeB4B61C

2. Virtual currency seized from unhosted virtual currency addresses, NFTs, and ENS domain names during the execution of seizure warrant 22-sz-13:

Unhosted Address Assets	**Amount**
Punk Vault (NFTX)	0.135126
USD Coin (USDC)	1,668.782899
SafeMoon Inu (SMI)	264,222,552.086639
UniCrypt (UNCX)	3.000000
Ethereum (ETH)	0.192765
Tether (USDT)	77.122725

Project Inverse (XIV)	3,000.000000

NFTs:
“Tender Morphism” 7/7
Gurlz Go Wildd #43
“Sweet Symphony” 10/10
Invisible Scissors #15
Invisible Scissors #86
Invisible Scissors #35

ENS Domain Names:
vhurryharry.eth
halfmooneye.eth

The above-listed assets were seized from the following unhosted addresses. These unhosted addresses are some of the “IT Worker Payment Addresses” and “IT Worker Consolidation Addresses,” as defined in the accompanying complaint.

- 0x44A9DaC239201DeF01B55dC8122cE1Dc8BD55C72
- 0x864C8ef839DD3859820BC6BcE450Aee43F938178
- 0x21A2CF2b1E84d9E9a38389F797F6087d94Ed3d86
- 0xf7bC1F442d436AFe5754b565bff030c281c9Aa90
- 0x3709d736F2615aE8e2f429e63aA3e1494b353D94
- 0xA184f953376A3c76A72A37849591ac6D8e148083
- 0xF17Cd87f477acE0BBb6Fe452bB50619c42AB4D97
- 0x7492FbBb52e58A0c3E1315f9b77a6b24e6414835

3. Virtual currency seized from two accounts at Binance during the execution of seizure warrant 22-sz-18:

Binance Account 369902286:

Asset	**Amount**
BTC	1.047995
USDT	200

Binance Account 126474093:

Asset	**Amount**
USDT	135

4. Virtual currency in the form of USDC frozen and U.S. dollars seized in connection with unhosted virtual currency addresses 0x815F335f976301f496167bfeF237f0622F92ac38 and 0x81c4d8816b29147c542dDE87485608204690Acf2 during the execution of seizure warrant 22-sz-19, which are some of the IT Worker Consolidation Addresses, as defined in the accompanying complaint:

Asset	**Amount**
USDC on Ethereum	187,035.41
USDC on Avalanche	31,584.20
USDC on Ethereum	12,262.25

5. Virtual currency in the form of USDT that was voluntarily frozen by Tether on or about September 1, 2022, in unhosted virtual currency addresses 0x815F335f976301f496167bfeF237f0622F92ac38 and 0x81c4d8816b29147c542dDE87485608204690Acf2, which are some of the IT Worker Consolidation Addresses, as defined in the accompanying complaint:

Asset	**Amount**
USDT on Ethereum	145,491.97
USDT on Ethereum	387,550.90

6. USDT that was voluntarily frozen by Tether on or about March 6, 2023, in unhosted virtual currency address 0x4F47Bc496083C727c5fbe3CE9CDf2B0f6496270c, which is SIM's Wallet, as defined in the accompanying complaint.

7. USDT that was voluntarily frozen by Tether on or about March 6, 2023, in unhosted virtual currency addresses 0x5707aA6944E357cEa1A25Ff991fB3A2E60268AB5 and

0xB389B4B4a8a6E267CA0712321cdca5c856ef8A72, which are some of the IT Worker Consolidation Addresses, as defined in the accompanying complaint.

8. USDT that was voluntarily frozen by Tether on or about April 1, 2023, in unhosted virtual currency addresses 0x15824de78A61a8B493CCd8A48e58463536B17028, 0x6E2F0deAB1C358547b353342524489e32640D530, 0x3E24F610639e105173003EF1c47dC4DbAa33f8D7, and 0x1c097e02bCd6cD69946663ace4bc0B115e256bAc, which are some of the IT Worker Consolidation Addresses, as defined in the accompanying complaint.

CIVIL COVER SHEET

JS-44 (Rev. 11/2020 DC)

I. (a) PLAINTIFFS

UNITED STATES OF AMERICA

(b) COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF ____________________
(EXCEPT IN U.S. PLAINTIFF CASES)

DEFENDANTS

VIRTUAL CURRENCY ASSOCIATED WITH NORTH KOREAN IT WORKER MONEY LAUNDERING AND SANCTIONS EVASION CONSPIRACIES

COUNTY OF RESIDENCE OF FIRST LISTED DEFENDANT ____________________
(IN U.S. PLAINTIFF CASES ONLY)
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED

(c) ATTORNEYS (FIRM NAME, ADDRESS, AND TELEPHONE NUMBER)

Rick Blaylock, Jr.
United States Attorney's Office
601 D Street, N.W., Washington, D.C. 20530
(202) 252-6765

ATTORNEYS (IF KNOWN)

II. BASIS OF JURISDICTION
(PLACE AN x IN ONE BOX ONLY)

● 1 U.S. Government Plaintiff
○ 3 Federal Question (U.S. Government Not a Party)
○ 2 U.S. Government Defendant
○ 4 Diversity (Indicate Citizenship of Parties in item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (PLACE AN x IN ONE BOX FOR PLAINTIFF AND ONE BOX FOR DEFENDANT) **FOR DIVERSITY CASES ONLY!**

	PTF	DFT		PTF	DFT
Citizen of this State	○ 1	○ 1	Incorporated or Principal Place of Business in This State	○ 4	○ 4
Citizen of Another State	○ 2	○ 2	Incorporated and Principal Place of Business in Another State	○ 5	○ 5
Citizen or Subject of a Foreign Country	○ 3	○ 3	Foreign Nation	○ 6	○ 6

IV. CASE ASSIGNMENT AND NATURE OF SUIT

(Place an X in one category, A-N, that best represents your Cause of Action and one in a corresponding Nature of Suit)

○ **A. *Antitrust***

□ 410 Antitrust

○ **B. *Personal Injury/ Malpractice***

□ 310 Airplane
□ 315 Airplane Product Liability
□ 320 Assault, Libel & Slander
□ 330 Federal Employers Liability
□ 340 Marine
□ 345 Marine Product Liability
□ 350 Motor Vehicle
□ 355 Motor Vehicle Product Liability
□ 360 Other Personal Injury
□ 362 Medical Malpractice
□ 365 Product Liability
□ 367 Health Care/Pharmaceutical Personal Injury Product Liability
□ 368 Asbestos Product Liability

○ **C. *Administrative Agency Review***

□ 151 Medicare Act

Social Security
□ 861 HIA (1395ff)
□ 862 Black Lung (923)
□ 863 DIWC/DIWW (405(g))
□ 864 SSID Title XVI
□ 865 RSI (405(g))

Other Statutes
□ 891 Agricultural Acts
□ 893 Environmental Matters
□ 890 Other Statutory Actions (If Administrative Agency is Involved)

○ **D. *Temporary Restraining Order/Preliminary Injunction***

Any nature of suit from any category may be selected for this category of case assignment.

(If Antitrust, then A governs)

● **E. *General Civil (Other)*** **OR** ○ **F. *Pro Se General Civil***

Real Property
□ 210 Land Condemnation
□ 220 Foreclosure
□ 230 Rent, Lease & Ejectment
□ 240 Torts to Land
□ 245 Tort Product Liability
□ 290 All Other Real Property

Personal Property
□ 370 Other Fraud
□ 371 Truth in Lending
□ 380 Other Personal Property Damage
□ 385 Property Damage Product Liability

Bankruptcy
□ 422 Appeal 27 USC 158
□ 423 Withdrawal 28 USC 157

Prisoner Petitions
□ 535 Death Penalty
□ 540 Mandamus & Other
□ 550 Civil Rights
□ 555 Prison Conditions
□ 560 Civil Detainee – Conditions of Confinement

Property Rights
□ 820 Copyrights
□ 830 Patent
□ 835 Patent – Abbreviated New Drug Application
□ 840 Trademark
□ 880 Defend Trade Secrets Act of 2016 (DTSA)

Federal Tax Suits
□ 870 Taxes (US plaintiff or defendant)
□ 871 IRS-Third Party 26 USC 7609

Forfeiture/Penalty
□ 625 Drug Related Seizure of Property 21 USC 881
☒ 690 Other

Other Statutes
□ 375 False Claims Act
□ 376 Qui Tam (31 USC 3729(a))
□ 400 State Reapportionment
□ 430 Banks & Banking
□ 450 Commerce/ICC Rates/etc
□ 460 Deportation
□ 462 Naturalization Application

□ 465 Other Immigration Actions
□ 470 Racketeer Influenced & Corrupt Organization
□ 480 Consumer Credit
□ 485 Telephone Consumer Protection Act (TCPA)
□ 490 Cable/Satellite TV
□ 850 Securities/Commodities/ Exchange
□ 896 Arbitration
□ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
□ 950 Constitutionality of State Statutes
□ 890 Other Statutory Actions (if not administrative agency review or Privacy Act)

○ **G. *Habeas Corpus/ 2255***

□ 530 Habeas Corpus – General
□ 510 Motion/Vacate Sentence
□ 463 Habeas Corpus – Alien Detainee

○ **H. *Employment Discrimination***

□ 442 Civil Rights – Employment (criteria: race, gender/sex, national origin, discrimination, disability, age, religion, retaliation)

(If pro se, select this deck)

○ **I. *FOIA/Privacy Act***

□ 895 Freedom of Information Act
□ 890 Other Statutory Actions (if Privacy Act)

(If pro se, select this deck)

○ **J. *Student Loan***

□ 152 Recovery of Defaulted Student Loan (excluding veterans)

○ **K. *Labor/ERISA (non-employment)***

□ 710 Fair Labor Standards Act
□ 720 Labor/Mgmt. Relations
□ 740 Labor Railway Act
□ 751 Family and Medical Leave Act
□ 790 Other Labor Litigation
□ 791 Empl. Ret. Inc. Security Act

○ **L. *Other Civil Rights (non-employment)***

□ 441 Voting (if not Voting Rights Act)
□ 443 Housing/Accommodations
□ 440 Other Civil Rights
□ 445 Americans w/Disabilities – Employment
□ 446 Americans w/Disabilities – Other
□ 448 Education

○ **M. *Contract***

□ 110 Insurance
□ 120 Marine
□ 130 Miller Act
□ 140 Negotiable Instrument
□ 150 Recovery of Overpayment & Enforcement of Judgment
□ 153 Recovery of Overpayment of Veteran's Benefits
□ 160 Stockholder's Suits
□ 190 Other Contracts
□ 195 Contract Product Liability
□ 196 Franchise

○ **N. *Three-Judge Court***

□ 441 Civil Rights – Voting (if Voting Rights Act)

V. ORIGIN

● 1 Original Proceeding
○ 2 Removed from State Court
○ 3 Remanded from Appellate Court
○ 4 Reinstated or Reopened
○ 5 Transferred from another district (specify)
○ 6 Multi-district Litigation
○ 7 Appeal to District Judge from Mag. Judge
○ 8 Multi-district Litigation – Direct File

VI. CAUSE OF ACTION (CITE THE U.S. CIVIL STATUTE UNDER WHICH YOU ARE FILING AND WRITE A BRIEF STATEMENT OF CAUSE.)

18 U.S.C. §§ 981(a)(1)(A) and 981(a)(1)(C)

VII. REQUESTED IN COMPLAINT □ CHECK IF THIS IS A CLASS ACTION UNDER F.R.C.P. 23 **DEMAND $** **JURY DEMAND:** Check YES only if demanded in complaint YES □ NO ☒

VIII. RELATED CASE(S) IF ANY (See instruction) **YES** □ **NO** ☒ If yes, please complete related case form

DATE: 6/5/2025 **SIGNATURE OF ATTORNEY OF RECORD** /s/ Rick Blaylock

INSTRUCTIONS FOR COMPLETING CIVIL COVER SHEET JS-44
Authority for Civil Cover Sheet

The JS-44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and services of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. Listed below are tips for completing the civil cover sheet. These tips coincide with the Roman Numerals on the cover sheet.

I. COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF/DEFENDANT (b) County of residence: Use 11001 to indicate plaintiff if resident of Washington, DC, 88888 if plaintiff is resident of United States but not Washington, DC, and 99999 if plaintiff is outside the United States.

III. CITIZENSHIP OF PRINCIPAL PARTIES: This section is completed only if diversity of citizenship was selected as the Basis of Jurisdiction under Section II.

IV. CASE ASSIGNMENT AND NATURE OF SUIT: The assignment of a judge to your case will depend on the category you select that best represents the primary cause of action found in your complaint. You may select only one category. You must also select one corresponding nature of suit found under the category of the case.

VI. CAUSE OF ACTION: Cite the U.S. Civil Statute under which you are filing and write a brief statement of the primary cause.

VIII. RELATED CASE(S), IF ANY: If you indicated that there is a related case, you must complete a related case form, which may be obtained from the Clerk's Office.

Because of the need for accurate and complete information, you should ensure the accuracy of the information provided prior to signing the form.