UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	
	)	**Civil Action No. 24-cv-2828**
APPROXIMATELY 1,694,395.463328 OF TETHER CRYPTOCURRENCY	)	
	)	
	)	
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 approximately 1,694,395.463328 of Tether cryptocurrency, 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), (b), and (c).

NATURE OF THE ACTION AND STATUTORY BASIS FOR FORFEITURE

3. The United States files this *in rem* forfeiture action to seek forfeiture of the Defendant Funds involved in, and constituting the proceeds of, violations of wire fraud, wire fraud conspiracy, money laundering, money laundering conspiracy, and computer fraud and abuse activity in violation of 18 U.S.C. §§ 2, 3, 1030, 1343, 1349, 1956(a)(1)(A)(i), 1956(h), and 1957.

4. Procedures for this action are mandated by Rule G of the supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions and, to the extent applicable, 18 U.S.C. §§ 981 and 983 and the Federal Rules of Civil Procedure.

5. 18 U.S.C. § 981(a)(1)(A) mandates forfeiture of any property, real or personal, involved in a transaction or attempted transaction in violation of section 18 U.S.C. §§ 1956, 1957 or 1960, or any property traceable to such property.

6. 18 U.S.C. § 981(a)(1)(C) mandates forfeiture of property constituting or derived from proceeds traceable to wire fraud, conspiracy to commit wire fraud, or any offense constituting "specified unlawful activity" as defined by 18 U.S.C. § 1956(c)(7), or a conspiracy to commit such offense. A violation of 18 U.S.C. §§ 1030 or 1343, or a conspiracy to commit that offense, constitutes specified unlawful activity under 18 U.S.C. § 1956(c)(7)(A) as an offense listed in 18 U.S.C. § 1961(1)(B).

7. Title 18 U.S.C. § 1030(a)(2) 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").

8. Title 18 U.S.C. § 1343 provides that whoever, having devised or intending to devise

any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, commits the violation of wire fraud.

9. Title 18 U.S.C. § 1349 provides that whoever attempts or conspires to commit a violation of 18 U.S.C. § 1343 shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy.

10. Title 18 U.S.C. § 1956(a)(1)(A)(i) provides in relevant part that whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity, knowing that the transaction is designed in whole or in part . . . to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity is guilty concealment money laundering.

11. Title 18 U.S.C. § 1956(h) provides that any person who conspires to commit any offense of 1956 or 1957 is subject to the same penalties as those prescribed for the offense the commission of which was the object of the conspiracy.

12. Title 18 U.S.C. § 1957 provides in relevant part that "[w]hoever . . . knowingly engages or attempts to engage in a monetary transaction in criminally derived property of a value greater than $10,000 and is derived from specified unlawful activity" is guilty of a federal offense. Because the offense consists of spending the proceeds of specified unlawful activity, section 1957 is sometimes called the Spending Statute. Violations of section 1957 are commonly referred to as money-laundering offenses.

PROPERTY INFORMATION

13. The Defendant Property consists of approximately 1,694,395.463328 in Tether, a virtual currency, seized from the following five virtual currency wallet addresses controlled by members of North Korean[1] military hacking groups known within the cybersecurity community as both the Lazarus Group and Advanced Persistent Threat 38 ("APT38"):

Defendant Property	Wallet Address	USDT Value
1	TF3JRez3XpJJYDCJ4hPtA1BTyxRurYsHTd	267,002
2	TBABZTh7p3tZGMnMefQkjqZuuyQK4iBCkS	504,883
3	TFeDK4Wea8ciDLaUe5W2QRSw9WvSqzV4p2	794,636
4	TT8WVp65uEJM4xdAkx2hJerQX5moeZYUEw	90,408
5	TN6iW22qfXM2c6L8amCvcGx3WcvTShvbMP	37,464

14. The Defendant Funds are currently in Federal Bureau of Investigation ("FBI") custody and will be transferred to the United States Marshals Service in the District of Columbia.

STATEMENT OF FACTS

15. The FBI is investigating several recent virtual currency heists perpetrated by North Korean military hacking groups, known within the cybersecurity community as both the Lazarus Group and APT38.[2] Since at least late-2014, North Korean cyber actors (hereinafter "NKCA") have

[1] The Democratic People's Republic of Korea is also known as "North Korea."

[2] APT or "Advanced Persistent Threat" is a term used to define and identify groups of organized, highly skilled, and well-resourced cyber actors who maintain focused efforts on specific tasks such as intelligence gathering against specific business sectors or governments. APTs are known to gain access to computer networks while remaining undetected for extended periods. APTs are often nation-state or state-sponsored groups. Upon identification, the group is assigned a unique number as an identifier by the community: in this case, the cybersecurity has dubbed this group of North Korean cyber actors as "APT38."

engaged in cyber-attacks, intrusions, and attempted intrusions into computers and networks of, among others, U.S. and foreign entertainment companies, U.S. and foreign banks, U.S. cleared defense contractors and energy companies, virtual currency exchanges, information security researchers, and pharmaceutical companies.

16. On or about November 1, 2022, NKCA stole virtual currency worth approximately $28 million dollars from COMPANY-1 and laundered it through decentralized virtual currency exchanges, a mixing service, and virtual currency bridges. The Defendant Property is traceable to the November 2022 hack and theft from COMPANY-1.

17. The United States of America seeks to lawfully forfeit the Defendant Property to punish and deter criminal activity by depriving criminals of property used in or acquired through illegal activities, to promote and enhance cooperation among law enforcement agencies, and most importantly: to recover assets that may be used to compensate victims.[3]

I. Background Related to Virtual Currency

18. **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

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

be used on other networks unless it is "wrapped" by smart contract code. This wrapping process results in what is called Wrapped ETH or WETH.

19. **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.

20. **Tether (hereinafter "USDT"):** Tether 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.

21. **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.

22. **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.

23. **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.

24. 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.

25. **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.

26. **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 API[4] 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.

27. **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.

28. **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

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

other.

29. **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).

30. **Virtual Currency Mixers:** Virtual currency mixers (also known as tumblers or mixing services) are software services that allow users, for a fee, to send virtual currency to designated recipients in a manner designed to conceal and obfuscate the source of the virtual currency. Virtual currency mixers are a common laundering tool used by North Korean cyber actors and their money laundering co-conspirators. As described below, Sinbad.io ("Sinbad") is one of the virtual currency mixers used in the Stake attack. On or about November 29, 2023, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) sanctioned Sinbad (for among other reasons) because it had been used to launder millions of dollars' worth of virtual currency from Lazarus Group heists, including the Harmony and Sky Mavis heists mentioned above.

31. **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

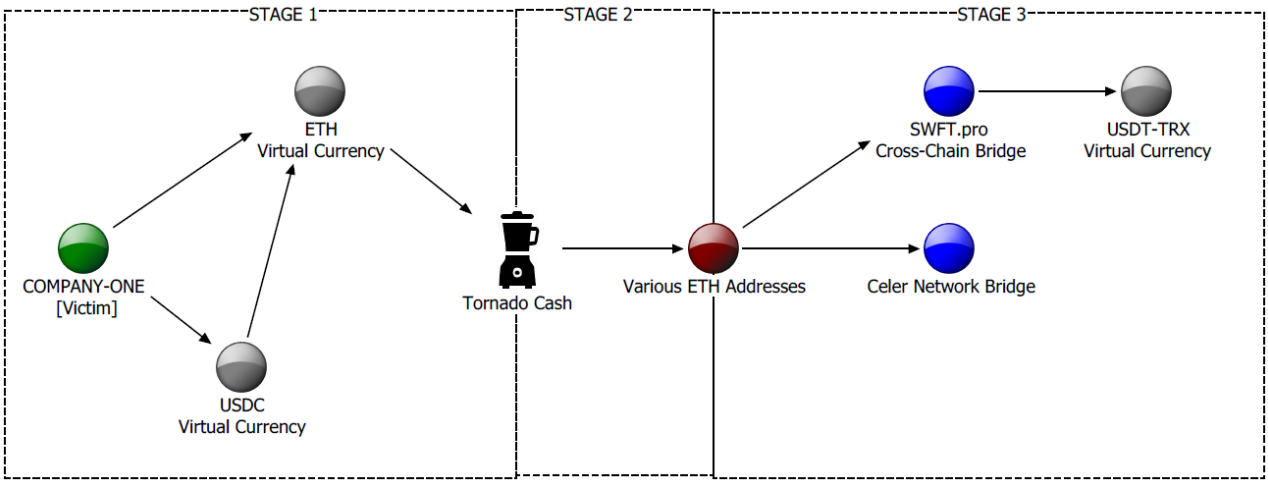
[BTC] address (*i.e.*, a "cluster"). It is possible to identify a 'cluster' of [BTC] addresses held by one organization by analyzing the [BTC] blockchain's transaction history. Open-source tools and private software products can be used to analyze a transaction." *United States v. Gratkowski*, 964 F.3d 307, 309 (5th Cir. 2020).

32. 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.

II. Cyberattack and Tracing of Funds

33. As previously stated, on or about November 1, 2022, NKCA stole approximately $28 million dollars' worth of virtual currency from COMPANY-1 and laundered it through decentralized virtual currency exchanges, a mixing service, and virtual currency bridges. The NKCA and co-conspirators laundered these stolen funds in three stages. **Stage 1** of the laundering involved the initial theft of USDC and ETH from COMPANY-1, the conversion of the stolen USDC to ETH via a decentralized exchange, and the deposit of stolen funds into an illicit virtual currency mixing service. **Stage 2** of the laundering involved moving the stolen funds out of the mixing service. **Stage 3** of the laundering involved the movement of funds through virtual currency bridges to convert the funds into USDT on the Tron network.[5] The virtual currency addresses containing USDT on the Tron network are the Defendant Properties. The following diagram depicts how the stolen ETH and USDC were laundered and eventually sent to the Defendant Properties:

[5] The diagram represents the virtual currency as USDT-TRX. TRX is the cryptocurrency used on the Tron network.



Laundering Stage 1

34. NKCA stole COMPANY-1's virtual currency on the Ethereum blockchain (both USDC and ETH) valued at approximately $14 million and sent it to virtual currency address 0x8d08aad4b2bac2bb761ac4781cf62468c9ec47b4 (0x8d08aa). NKCA then converted stolen USDC tokens to ETH, the native coin of the Ethereum blockchain, through a decentralized exchange. This meant that the NKCA (and/or their money laundering co-conspirators) now had only ETH to launder, not ETH and USDC. Money launderers attempt to convert centrally managed assets, such as USDC, to those that are decentralized to make it harder for law enforcement to freeze and seize the assets. The stolen ETH, amounting to approximately 9,109 ETH, was then transferred to Ethereum address 0xb0606f433496bf66338b8ad6b6d51fc4d84a44cd (0xb0606f) and to Ethereum address 0x3089df0e2349faea1c8ec4a08593c137da10fe2d (0x3089df). The NKCA then transferred from 0xb0606f and 0x3089df the approximately 9,109 ETH to Tornado Cash, an Ethereum-based virtual currency mixing service, on or about November 5 and November 7, 2022.

Laundering Stage 2

35. Tornado Cash is a mixing service that operates on the Ethereum blockchain. Users of Tornado Cash can only deposit ETH into Tornado Cash via different "pools" that allow for transfer

in increments of 0.1 ETH, 1 ETH, 10 ETH and 100 ETH. On or about November 5, 2022, and November 7, 2022, the NKCA initiated approximately 90 transfers of ETH, or 9,000 ETH, into the Tornado Cash 100 ETH pool.

36. Although mixing services are used to obfuscate the trail of funds, law enforcement can sometimes trace the funds in and out—as they did here. In reviewing withdrawals made during November of 2022 from the Tornado Cash 100 ETH pool, law enforcement observed various connections among seventeen different Ethereum addresses (the "Tornado Cash Withdrawal Addresses").[6] These connections, as further described below in "Laundering Stage 3," included (1) the timing of transfers (some within minutes of each other), (2) the use of the same virtual currency cross-chain bridging services (such as Celer Network Bridge and SWFT.pro), (3) stolen funds being transferred to the same blockchain (the Tron blockchain), (4) certain transaction fees being funded by the same address, and (5) virtual currency on the Tron blockchain being sent to the same consolidation address, TCxWVTbtoqLbthFrdyyJ6cV8aK5UXXBnbS (TCxWVTb). The Tornado Cash Withdrawal Addresses received 78 withdrawals from the Tornado Cash 100 ETH pool (or 7,800 ETH) beginning on or about November 7, 2022.

37. The deposits into the Tornado Cash 100 ETH pool that funded the 7,800 ETH received by the Tornado Cash Withdrawal Addresses would have been deposited within seven days of the withdrawal. An analysis conducted by the FBI of all deposits into the Tornado Cash 100 ETH pool from on or about November 1, 2022, to November 7, 2022, revealed that 75 percent, or approximately 9,000 ETH of the total approximately 12,000 ETH, were traced back to funds stolen

[6] The Tornado Cash Withdrawal Addresses are included in the "Various ETH Addresses" in the chart above. The stolen funds were transferred from the Tornado Cash Withdrawal Addresses to other Ethereum addresses throughout the laundering process, and therefore the "Various ETH Addresses" include a larger number of addresses.

from COMPANY-1 and laundered as described in Laundering Stage 1. The other approximately 25 percent - approximately 3,000 ETH of the approximately 12,000 ETH - represented funds from other Tornado Cash users who sought to have their funds mixed. Based upon the analysis of deposits and withdrawals into the Tornado Cash 100 ETH pool described above, the 7,800 ETH received by the Tornado Cash Withdrawal Addresses were funded by COMPANY-1 stolen funds described in Laundering Stage 1.

Laundering Stage 3

38. As described above, once the stolen funds were withdrawn from Tornado Cash, the NKCA (and/or their money laundering co-conspirators) used a variety of services to convert the stolen funds to USDT on the Tron blockchain. These transfers occurred in three different waves, separated by assets being frozen by law enforcement.

Wave 1

39. Seven of the 17 Tornado Cash Withdrawal Addresses received approximately 3,000 ETH of the approximately 7,800 ETH described in Laundering Stage 2. Through intermediary Ethereum addresses, these seven Ethereum addresses converted this approximately 3,000 ETH to USDT on the Ethereum blockchain. Between on or about January 6, 2023, and January 20, 2023, this USDT on the Ethereum blockchain was transferred to USDT on the Tron blockchain via SWFT.pro, a cross-chain bridging service. This stolen USDT was received by seven different Tron addresses. These Tron addresses were all funded by TRX, the native token on the Tron blockchain, from the same Tron address, TVaV2BBs8tpthbp19QAy7ibmXLoYsomKDD (TVaV2BB), for the purpose of paying gas fees.[7] These seven Tron addresses then transferred USDT to seven different

[7] On the Tron blockchain, tokens, also known as TRC-20 tokens, are created and can be transferred between different addresses on the Tron blockchain. An example of a TRC-20 token is USDT. These TRC-20 tokens can be transferred by an owner of a Tron address by paying transaction fees, also

Tron addresses, namely:

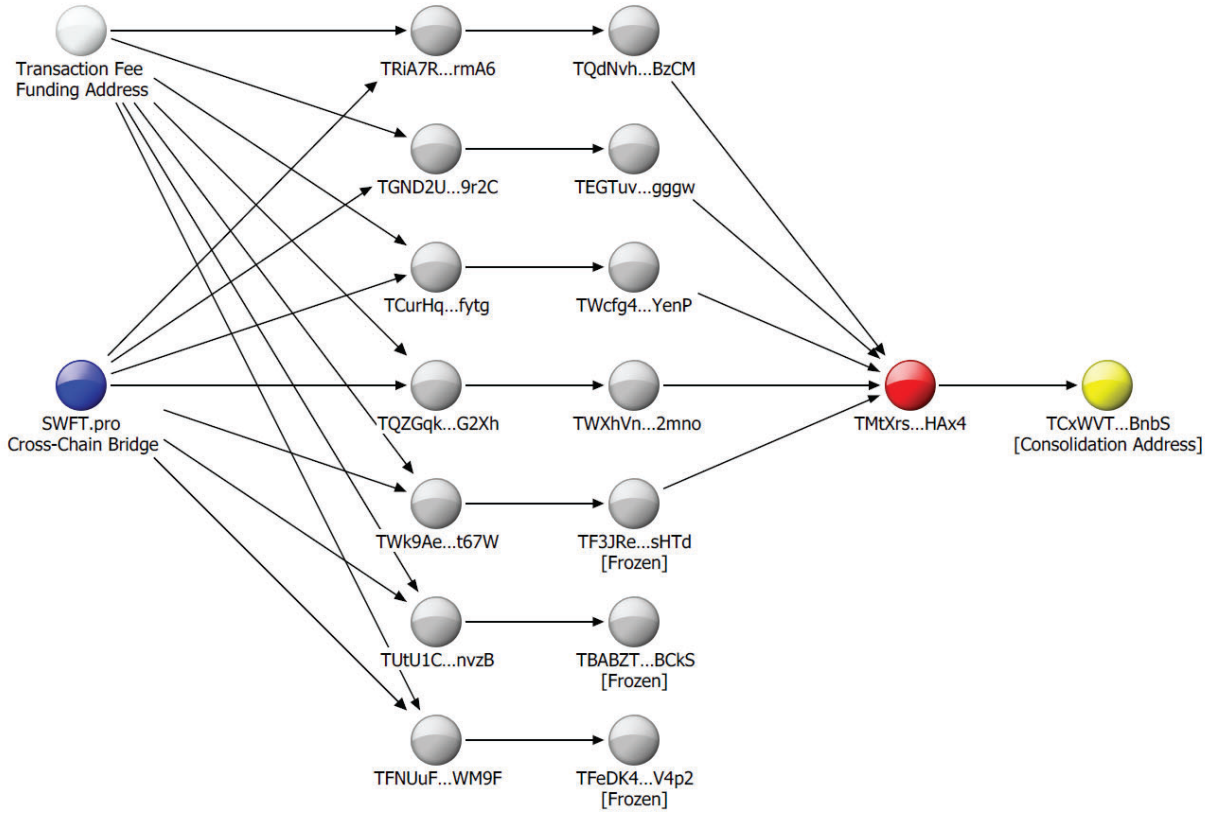
Address #	**Address**
1	TQdNvhGKQtVKNhBSJ1xbisxiNxUCgPBzCM
2	TEGTuvMgEMcLP21GLa3XUCSsgZn4pbgggw
3	TWcfg4q4wH36J5R4Au8KnPFrxcrQd1YenP
4	TWXhVnNi4bUiii7g13YyWQuR1gacsp2mno
5	TF3JRez3XpJJYDCJ4hPtA1BTyxRurYsHTd (Defendant Property 1)
6	TBABZTh7p3tZGMnMefQkjqZuuyQK4iBCkS (Defendant Property 2)
7	TFeDK4WEa8ciDLaUe5W2QRSw9WvSqzV4p2 (Defendant Property 3)

Addresses 1 through 5 of the above Tron addresses sent some or all of their funds, directly or indirectly, to the same consolidation address: TCxWVTb. Between on or about January 20, 2023, and January 25, 2023, the following addresses were frozen:

known as gas fees. These gas fees can only be paid via TRX, the native token on the Tron blockchain. Therefore, analysis showing the transfer of TRX (*i.e.*, the gas needed to make the transactions happen) to these addresses that received USDT from the same Tron address further establishes a connection between these Tron addresses.

Defendant Property #	Address	Approx. Value
1	TF3JRez3XpJJYDCJ4hPtA1BTyxRurYsHTd	267,002 USDT
2	TBABZTh7p3tZGMnMefQkjqZuuyQK4iBCkS	504,883 USDT
3	TFeDK4Wea8ciDLaUe5W2QRSw9WvSqzV4p2	794,636 USDT

These addresses are three of the five Defendant Properties. The below diagram shows the flow of COMPANY-1 stolen funds through Wave 1, beginning with SWFT.pro and showing three Defendant Properties, the gas funding address, and the Consolidation Address.



Wave 2

40. After the above USDT was frozen, the NKCA modified their techniques for converting stolen assets to USDT on Tron. Beginning on or about February 27, 2023, five of the

Tornado Cash Withdrawal Addresses transferred approximately 3,100 ETH to five different Ethereum addresses. These transfers all occurred within approximately 10 minutes. The majority of these funds were ultimately transferred to the Tron blockchain, many times after utilizing multiple cross-chain bridges, including SWFT.pro and Celer Network. The movement of stolen funds in this manner represents laundering activity because the use of multiple services in this way is an attempt to obfuscate the location of the stolen funds.

41. Stolen funds from the five Tornado Cash Withdrawal Addresses described above were transferred, by the techniques described above, to approximately thirty-two different Tron addresses. Many of these stolen funds were sent to the same consolidation address which received the stolen funds in Wave 1 and described above, TCxWVTb.

42. Between on or about March 22, 2023, and March 29, 2023, two of the thirty-two Tron addresses were frozen:

Defendant Property #	**Address**	**Approx. Value**
4	TT8WVp65uEJM4xdAkx2hJerQX5moeZYUEw	90,408 USDT
5	TN6iW22qfXM2c6L8amCvcGx3WcvTShvbMP	37,464 USDT

Wave 3

43. After funds were frozen as described in the paragraph above, the NKCA again modified their techniques for laundering stolen funds. The FBI has not been able to freeze any assets through Wave 3, however, the following facts are included herein to further show the connections between the Tornado Cash Withdrawal Addresses laundered through Wave 1 and Wave 2.

44. From on or about April 27, 2023, to May 8, 2023, stolen funds that were received by the final five Tornado Cash Withdrawal Addresses were transferred to approximately 14 different

addresses on the Tron blockchain. These transfers occurred in the same pattern as described above, utilizing Celer Network Bridge to different blockchains before being transferred to Tron through the SWFT.pro cross-chain bridge. Many of these funds were sent to the same consolidation address on the Tron blockchain, TR6RGkw4aMAUgTTMmCrNLA41urrLBLH3BF (TR6RGkw). TR6RGkw received funds from one of the Tron addresses that received funds during the second wave of laundering described above. Additionally, TR6RGkw sent approximately 628,320 USDT to TCxWVTb, which was the same consolidation address utilized in the first two waves of laundering described above. No assets were frozen during Wave 3.

III. Seizure of Defendant Funds

45. On or about April 1, 2024, the Department of Justice served a federal seizure warrant for the Defendant Property.

46. The Defendant Property is currently in the possession of the United States.

COUNT ONE – FORFEITURE OF DEFENDANT PROPERTY

(18 U.S.C. §§ 981(a)(1)(C))

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

48. The Defendant Funds are property constituting or derived from proceeds traceable to wire fraud and conspiracy to commit wire fraud, in violation of 18 U.S.C. §§ 1030, 1343, and 1349.

49. Accordingly, the Defendant Funds are subject to forfeiture to the United States under 18 U.S.C. § 981(a)(1)(C).

COUNT TWO – FORFEITURE OF DEFENDANT PROPERTY

(18 U.S.C. §§ 981(a)(1)(A))

50. Paragraphs 1 through 46 are realleged and incorporated by reference here.

51. The Defendant funds are property involved in a transaction or attempted transaction in violation of 18 U.S.C. §§ 1956(a)(1)(B)(i), 1956(a)(2)(B)(i), 1956(h), and 1957, that is, a

conspiracy to conduct or attempt to conduct financial transactions involving the proceeds of specified unlawful activity, to wit, wire 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; and a conspiracy to knowingly engage in or attempt to engage in monetary transactions in criminally derived property of a value greater than $10,000 derived from specified unlawful activity, to wit, wire fraud and conspiracy to commit wire fraud.

52. Accordingly, the Defendant Funds are subject to forfeiture to the United States under 18 U.S.C. § 981(a)(1)(A).

PRAYER FOR RELIEF

WHEREFORE, the United States of America prays that notice issue on the Defendant Property as described above; that due notice be given to all parties to appear and show cause why the forfeiture should not be decreed; that this Honorable Court issue a warrant of arrest *in rem* according to law; that judgment be entered declaring that the Defendant Property be forfeited to the United States of America for disposition according to law; and that the United States of America be granted such other relief as this Court may deem just and proper.

October 4, 2024
Washington, D.C.

Respectfully submitted,

MATTHEW M. GRAVES
United States Attorney
D.C. Bar No. 481052

/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

/s/ Jessica C. Peck
Jessica C. Peck
N.Y. 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)

/s/ Maxwell Coll
Maxwell Coll
CA Bar No. 312651
Trial Attorney
Computer Crime & Intellectual Property Section
Criminal Division
U.S. Department of Justice
1301 New York Avenue, N.W.
Washington, D.C. 20005
(213) 894-1785
maxwell.coll@usdoj.gov

/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
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530
Telephone: 202-353-4273
Email: Gregory.Nicosia@usdoj.gov

VERIFICATION

I, Matt Richter, 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 3rd day of October, 2024.

Matt Richter
Special Agent
Federal Bureau of Investigation