UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	
	)	**Civil Action No. 24-cv-2826**
BITCOIN AND BTC.B SEIZED FROM EIGHT TRANSACTION HASHES AT CRYPTOCURRENCY BRIDGE-1	)	
	)	
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 Bitcoin and BTC.b Seized from Eight Transaction Hashes at Cryptocurrency Bridge-1, hereinafter the Defendant Funds, 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 STATURY 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 Funds are virtual currency stored within, or associated with, the following transaction hashes, controlled by Cryptocurrency Bridge-1, a U.S.-based company:

Number	Transaction Hash	Amount
Transaction Hash 1	0x40c1ab9902d4d811fef905057467056c56 5b6680ba5d28e198f632c1a251411a	.005 BTC.b
Transaction Hash 2	0xb531dfd0c5db681ccdac5c1837560e1b63 7b2209a1765387002938def591d9fb	3.20963359 BTC.b
Transaction Hash 3	0xc8a598cd90935eb0169b9960c5d06d102f ccb410a06b2ea77b20f6c8bb3d1c34	6.41403422 BTC.b
Transaction Hash 4	0xa62bca819ef4960b74363c3724471692f6 1145a132d3da8032973095038e50e7	5.32860588 BTC.b
Transaction Hash 5	0x187d936949a969caa91c22217762c4845d 9e17269bf0e92921508125012ea6bc	0.05 BTC.b
Transaction Hash 6	0x78c2fb0edd338e39e307ef448bef3f9459f bf7f1a05e2613b2ae054ed1fa28db	0.41283124 BTC.b
Transaction Hash 7	0x759e14f4007881d7cc8b808733c3247bd1 26a929b4bf01d0fdbab448177c1703	0.01885531 BTC.b
Transaction Hash 8	53405215888a8a71d5b67d85835050d721a 5df56b8e89fb4a567325daa253501	0.09997936 BTC

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 members of North Korean military hacking groups known within the cybersecurity community as both the Lazarus Group and APT38.[1] As is relevant for purposes of this filing, in or around August 2021, North Korean cyber actors stole approximately $90 million in virtual currency from COMPANY-1, a Japan-based virtual currency exchange. Next, in or around March 2022, North Korean cyber actors stole approximately $615 million in virtual currency from foreign-based COMPANY-2. Then, in or around June 2022, North Korean cyber actors stole approximately $105 million in virtual currency from COMPANY-3, a U.S.-based company. Finally, on or about September 4, 2023, North Korean cyber actors hacked and stole approximately $41 million worth of virtual currency from COMPANY-4.

16. The Defendant Funds are traceable to the September 2023 hack and theft of funds from COMPANY-4.

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

[1] 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."

illegal activities, to promote and enhance cooperation among law enforcement agencies, and most importantly: to recover assets that may be used to compensate victims.[2]

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 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 (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.

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

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 the instant complaint 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[3] 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 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 on their

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

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

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. Based on my training and experience, I know that 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 COMPANY-4 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. "For example, when 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. COMPANY-4 Cyberattack and Tracing of Funds

33. As previously stated, on or about September 4, 2023, North Korean hackers gained unauthorized access to COMPANY-4's computer systems and stole approximately $41 million dollars' worth of virtual currency from COMPANY-4. Thereafter, the North Koreans and their money laundering co-conspirators transferred the stolen funds through virtual currency bridges, several BTC addresses, and virtual currency mixers before consolidating funds and depositing the virtual currency at different virtual currency exchanges. **Stage 1** of the laundering involved the initial theft from COMPANY-4 and the conversion of stolen funds into BTC through bridging networks. **Stage 2** of the laundering involved moving the stolen BTC through virtual currency mixing services. **Stage 3** of the laundering involved the movement of post-mixer BTC into virtual currency exchanges and then the conversion of that post-mixer BTC to stablecoins, such as USDT.

34. The Defendant Funds represented in Transaction Hashes 1 through 7 in paragraph 13 above were seized during Stage 1 of the laundering. The Defendant Funds represented in Transaction Hash 8 were seized during Stage 3 of the laundering. All of the Defendant Funds were seized from Cryptocurrency Bridge-1.

A. *Stage 1: Use of Virtual Currency Bridges to Convert Stolen Funds to BTC*

35. North Korean hackers stole some of COMPANY-4's virtual currency from the Polygon Network. At the time of the hack, those the stolen funds were valued at approximately $7.8 million. (The Polygon Network is a blockchain similar to the Ethereum blockchain.) The North

Korean hackers then converted centrally managed stablecoins, like USDT, to MATIC, the coin native to the Polygon Network, through a decentralized virtual currency exchange.

36. North Korean hackers also stole some of COMPANY-4's virtual currency from the Binance Smart Chain ("BSC"). At the time of the hack, those stolen funds were valued at approximately $17.8 million. (The BSC is a blockchain similar to the Ethereum blockchain.) North Korean hackers then converted stolen tokens to BNB, the coin native to the BSC, through a decentralized exchange.

37. North Korean hackers also stole some of COMPANY-4's virtual currency from the Ethereum network. At the time of the hack, those stolen funds were valued at approximately $15.7 million. North Korean hackers then converted the stolen tokens, including centrally managed stablecoins, to ETH, the native coin of the Ethereum blockchain, through a decentralized exchange.

38. The North Korean hackers then began a process of moving the stolen assets from the Polygon Network, the BSC, and the Ethereum network to the BTC blockchain. The North Korean hackers used a variety of virtual currency bridges to accomplish this conversion to BTC, including Cryptocurrency Bridge-1.

39. The United States successfully froze the Defendant Funds during the North Korean hackers' use of Cryptocurrency Bridge-1. Specifically:

a. **Transaction Hashes 1 and 2**: On or about September 7, 2023, North Korean hackers transferred 550,000 MATIC coins to an address on the Polygon Network and then to Cryptocurrency Bridge-1. From this pool of funds, a portion of the MATIC coins were converted in two separate transactions to .005 BTC.b and 3.20963359 BTC.b, which were frozen at Cryptocurrency Bridge-1.

b. **Transaction Hashes 3 and 4**: On or about September 7, 2023, North Korean hackers transferred another 550,000 MATIC coins to a second address on the Polygon Network and then to Cryptocurrency Bridge-1. From this pool of funds, a majority of the MATIC coins were converted in two separate transactions to 6.414 BTC.b and 5.328 BTC.b, which were frozen at Cryptocurrency Bridge-1.

c. **Transaction Hash 5**: On or about September 7, 2023, North Korean hackers transferred another 600,000 MATIC coins to a third address on the Polygon Network and then to Cryptocurrency Bridge-1. From this pool of funds, some of the MATIC coins were converted in one transaction to .05 BTC.b, which was frozen at Cryptocurrency Bridge-1.

d. **Transaction Hashes 6 and 7**: On or about September 11, 2023, North Korean hackers transferred 300 BNB to an address on the on BSC blockchain and then to Cryptocurrency Bridge-1. From this pool of funds, some of the BNB was converted in two separate transactions to 0.412 BTC.b and 0.01885531 BTC.b, which were frozen at Cryptocurrency Bridge-1.

B. ***Stage 2: Use of Virtual Currency Mixers to Obfuscate Stolen Funds***

40. Although certain transactions were frozen while North Korean hackers were attempting to transfer stolen assets from the Ethereum, Polygon, and BSC blockchains, the North Koreans were able to transfer the majority of the stolen funds to the BTC blockchain.

41. Once on the BTC blockchain, the stolen assets were then sent through two different virtual currency mixing services designed to obfuscate the source of the stolen funds. These services were Sinbad and Yomix.

42. Sinbad allows a customer to pick the number of output addresses they want the mixed funds to be delivered to, which can be up to eight addresses. Sinbad also allows up to seven days for the customer to withdraw the funds from the mixer, and the fee ranges from 0.5% to 2.5%. Sinbad

typically utilized only bech32 addresses (i.e., BTC addresses beginning with bc1q), along with three or four outputs in a transaction.

43. Yomix offers several features, such as up to five output addresses to receive mixed funds, instant mixing if a delay is not set, and the ability to withdraw funds up to three days after sending them to be mixed. The minimum fee paid to Yomix is 0.7%.

44. Law enforcement traced the flow of the stolen funds through both mixing services to the next stage of the North Korean hackers' laundering process.

C. *Stage 3: Movement of Post-Mixer BTC to VCEs and Stablecoins*

45. Relevant to the instant complaint, on or about November 1, 2023, the North Korean hackers began consolidating funds that were mixed using one of the mixing services. The funds were consolidated at the following address: bc1q9wk2jtnex6wxsmkmp66azearfh8cryvyrg6rnr.

46. **Transaction Hash 8:** On or about November 3, 2023, the North Korean hackers attempted to send assets originating from bc1q9wk2jtnex6wxsmkmp66azearfh8cryvyrg6rnr on the BTC blockchain back to Cryptocurrency Bridge-1, including .099 BTC that was frozen at Cryptocurrency Bridge-1.

III. Seizure of the Defendant Funds

47. On or about February 9, 2024, the Department of Justice served a federal seizure warrant for the Defendant Funds on Cryptocurrency Bridge-1 and caused the transfer of the Defendant Funds to the United States.

48. The Defendant Funds are currently in the possession of the United States.

COUNT ONE – FORFEITURE OF DEFENDANT PROPERTY

(18 U.S.C. §§ 981(a)(1)(C))

49. Paragraphs 1 through 48 are realleged and incorporated by reference here.

50. 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.

51. 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))

52. Paragraphs 1 through 48 are realleged and incorporated by reference here.

53. 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.

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

PRAYER FOR RELIEF

55. 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

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)

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

VERIFICATION

I, Justin M. Vallese, 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.

Justin Vallese
Special Agent
Federal Bureau of Investigation