

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA,)	
)	
Plaintiff,)	
)	
v.)	
)	Civil Action No. 24-cv-3375
APPROXIMATELY 2210.8222 OF)	
SOL 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 2210.8222 of Solana (“SOL”) cryptocurrency, hereinafter the “Defendant Property,” and alleges as follows:

JURISDICTION AND VENUE

1. Seizures are appropriate from this district, because, as of the writing of this affidavit, the evidence has established that the criminal offenses under investigation were begun or committed upon the high seas, or elsewhere out of the jurisdiction of any particular State or district, and no offender is known to have, or have had, residence within any United States district. *See* 18 U.S.C. § 3238.

STATUTORY AUTHORITY

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

3. **Computer fraud and abuse:** 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”).

4. 18 U.S.C. § 371 prohibits a conspiracy to commit an offense or to defraud the United States, including a violation of 18 U.S.C. § 1030(a)(2).

5. **Wire fraud:** 18 U.S.C. § 1343 makes it a crime for anyone, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, to transmit or cause to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice. 18 U.S.C. § 1349 prohibits the attempt or conspiracy of a violation of 18 U.S.C. § 1343.

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

activity. This offense is sometimes referred to as promotional money laundering. 18 U.S.C. § 1956(a)(1)(B)(i) makes it a crime to conduct or attempt to conduct a financial transaction, knowing that the property involved in the transaction represents the proceeds of some form of unlawful activity, and which in fact involves the proceeds of specified unlawful activity, knowing that the transaction is designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity. This offense is sometimes referred to as concealment money laundering.

7. The term “specified unlawful activity” is defined in 18 U.S.C. §§ 1956(c)(7) and 1961(1), and it includes violations of 18 U.S.C. § 1030 (Computer fraud and abuse), and 18 U.S.C. § 1343 (Wire fraud).

8. 18 U.S.C. § 1956(h) criminalizes a conspiracy to violate § 1956.

9. Forfeiture Statutes. Pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c), any property, real or personal, which constitutes or is derived from “proceeds” traceable to a violation of 18 U.S.C. § 1030 (Computer fraud and abuse), 18 U.S.C. § 1343 (Wire fraud), or a conspiracy to commit such an offense, is subject to criminal and civil forfeiture.

10. Pursuant to 18 U.S.C. § 982(a)(1) and 18 U.S.C. § 981(a)(1)(A), any property, real or personal, “involved in” a transaction or attempted transaction in violation of 18 U.S.C. § 1956 (Money laundering) is subject to criminal and civil forfeiture. Forfeiture pursuant to these statutes applies to more than just the proceeds of the crime. These forfeitures encompass all property “involved in” the crime or the attempted crime, which can include “clean” or “legitimate” money that is commingled with “tainted” money derived from illicit sources. This commingling is a laundering technique that facilitates the scheme because it obfuscates the trail of the illicit funds. *See, e.g., United States v. Huber*, 404 F.3d 1047, 1058 (8th Cir. 2005) (the presence of legitimate

funds does not make a money laundering transaction lawful; it is only necessary to show that the transaction involves criminal proceeds).

11. 18 U.S.C. § 981(b) states that property subject to forfeiture under Section 981 may be seized via a civil seizure warrant issued by a judicial officer “in any district in which a forfeiture action against the property may be filed,” and may be executed “in any district in which the property is found,” if there is probable cause to believe the property is subject to forfeiture. 18 U.S.C. § 982(b)(1) incorporates the procedures in 21 U.S.C. § 853 (other than subsection (d)) for all stages of a criminal forfeiture proceeding. Section 853 permits the government to request the issuance of a seizure warrant for property subject to criminal forfeiture. Seizures are appropriate from this district, because the criminal offenses under investigation were begun or committed upon the high seas, or elsewhere out of the jurisdiction of any particular State or district, and no offender is known to have, or have had, residence within any United States district. *See* 18 U.S.C. § 3238.

DEFINITIONS AND BACKGROUND

Background Related to Virtual Currency

12. **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 are 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. For instance, ETH (the native token on the Ethereum network) cannot be used on other networks unless it is “wrapped” by smart contract code.

13. **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.

14. **Virtual Currency Address:** Virtual currency addresses are the 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.

15. **Private Keys:** Each virtual currency address is controlled using 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.

16. **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.

17. 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.

18. **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.

19. **Blockchain Explorer:** These explorers are online tools that operate as a blockchain search engine allowing users the ability to search for and review transactional data for any addresses on a particular blockchain. A blockchain explorer is software that uses application programming interface (API) 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. An API is a set of definitions and protocols for building and integrating application software.

20. **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.

21. **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.

22. **Virtual Currency Exchange (VCEs):** VCEs are trading and/or storage platforms for virtual currencies (*e.g.*, 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).

23. **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.

24. **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).

25. 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.

Background Regarding FBI's Lazarus Group Investigation

26. The FBI is investigating virtual currency hacks perpetrated by members of a North Korean military hacking group known within the cybersecurity community as the Lazarus Group or APT38.¹ The FBI assesses that Lazarus Group/APT38 actors are responsible for these hacks based on, among other things, distinctive tactics, techniques, and procedures observed in virtual currency heists linked to North Korea. Since at least late 2014, these subjects have 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. These North Korean subjects have exhibited a particular focus on leveraging their malicious cyber activity to steal money and virtual currency from their victims. From at least 2017 through 2024, the North Korean subjects continued this targeting and successfully conducted multiple virtual currency heists from virtual asset service providers and other victims, netting hundreds of millions of dollars of virtual currency.

27. To effectuate some of their hacking activity, Lazarus Group actors conduct social-engineering campaigns, frequently via LinkedIn, to compromise employees at virtual currency-related companies. These actors use multiple personas and purport to be recruiters from well-

¹ APT is an acronym for “Advanced Persistent Threat” and is 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, APT38.

known companies within the industry. After some high-level business discussions and rapport building, the actors will request that the victims continue the discussion through other communication methods, such as WhatsApp, Telegram, or Slack. As a part of the interview, the victims are convinced to execute a project from a GitHub repository that is malicious in nature. In other words, the victims are convinced to download malware onto their computer without knowing it. Once the victims (i.e., the targeted employees) are compromised, the actors will try to obtain credentials to access the company's infrastructure and obtain the private keys to virtual asset holdings. The FBI refers to this particular type of Lazarus Group activity as "TraderTraitor."

Background Regarding the Rain.com Theft

28. Rain Management W.L.L., also known as Rain.com, is licensed by the Central Bank of Bahrain as a Category 3 Crypto-Asset Services Provider.² As a Crypto-Asset Service Provider, Rain.com offers its customers the ability to swap between different currencies, purchase or sell virtual currency, manage customer's portfolios and assist with investment decisions. Rain Management is headquartered in the Kingdom of Bahrain.

29. On or about April 29, 2024, Rain.com was targeted by TraderTraitor malware, which the FBI knows to be associated with APT38. That targeting resulted in a financial loss to Rain.com of approximately \$16.13 million, including approximately \$760,997.68 in SOL.³ As described in more detail below, of the \$16.13 million stolen, the FBI was able to successfully

² A category 3 license allows a crypto-asset service, in this case Rain.com, to undertake certain virtual currency services. The description of categories is listed on the Central Bank of Bahrain's Rulebook.

³ Solana is a blockchain platform. Similar to other blockchains, it is designed to host decentralized, scalable applications. It varies from other blockchains by the cost, transaction rates, and transaction fees.

freeze 2210.8222 SOL at WhiteBIT, a virtual currency exchange headquartered in Vilnius, Vlinias Apskritis, Lithuania.

Rain.com's Response to the Theft

30. In sum, Rain.com conducted an internal investigation. That investigation revealed that actors gained unauthorized access to Rain.com's virtual currency using one of North Korea's signature malware strains, TraderTraitor. According to Rain.com, the infiltration only enabled the exploitation of the Rain.com "send" wallets. A "send" wallet likely refers to Rain.com's "hot wallet" used to send money to customers. A hot wallet is a key storage method for any private key that is connected either directly to the internet or through another device.

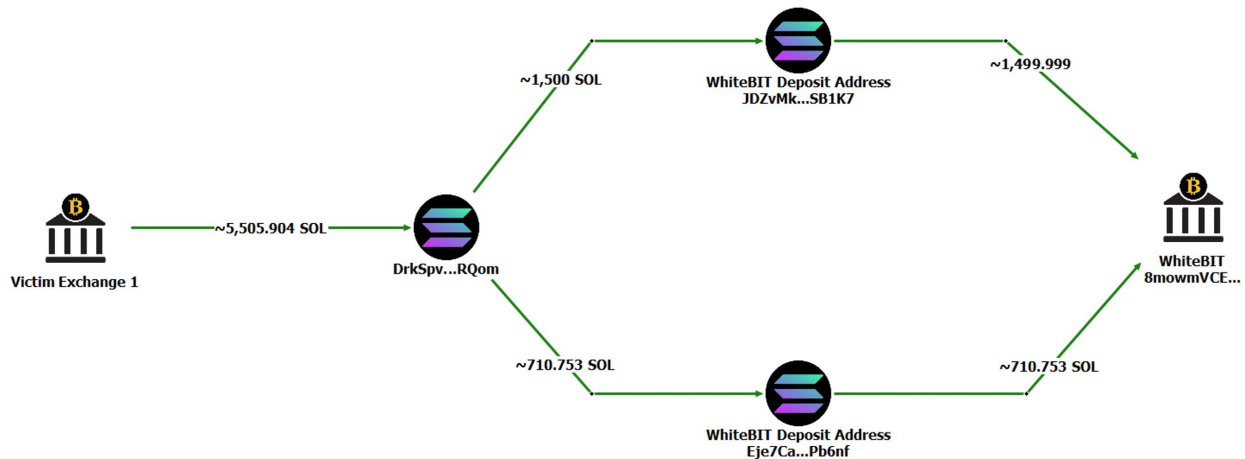
31. After the theft, Rain.com hired Mandiant Inc.⁴ ("Mandiant") to investigate the cybersecurity breach. When conducting their investigation, Mandiant learned that a Rain.com employee ("Employee 1") was compromised. Specifically, based on the investigation to date, law enforcement assesses that North Korean cyber actors contacted Employee 1 on LinkedIn and asked if Employee 1 was interested in a new job. Employee 1 indicated that Employee 1 was interested, so the North Korean cyber actors sent Employee 1 a malicious link disguised as a coding challenge. When Employee 1 downloaded the coding challenge, Employee 1's device was compromised with malware. This malware allowed the North Korean actors to steal private keys and credentials that ultimately gave the actors access to Rain.com's infrastructure managed by BitGo.⁵ That was important because Rain.com used BitGo to interact with and manage Rain.com's virtual currency assets and infrastructure. After the foothold was established via Employee 1, the North Korean actors stole virtual currency from Rain.com and deleted the malware from Employee 1's device.

⁴ Mandiant Inc. is a U.S. cybersecurity firm and a subsidiary of Google.

⁵ BitGo is a digital asset security and custody company located in Palo Alto, California.

32. The funds that are the subject of this warrant were traced from Rain.com’s wallets to WhiteBIT, where they were frozen pending seizure.

33. Below is a graph, created by the FBI, of the transactions involved in the theft through the deposit of stolen funds at the WhiteBIT exchange:



Details Regarding Tracing the Stolen Funds to WhiteBIT

34. FBI investigators traced a total of eight transactions involving funds stolen from Rain.com’s hot wallet to an address controlled by the North Korean cyber actors and/or their money laundering co-conspirators, “**DrkSpv...RQom**.” Beginning on or about April 29, 2024, at 01:54 GMT, and continuing through 03:42 GMT, through these eight transactions, the actors stole 5,505.904159384 SOL, which was valued at approximately \$760,997.68 as of the date of the theft.

35. Of the 5,505.904159384 SOL sent to address “**DrkSpv...RQom**,” approximately 4,890 SOL was sent in seven transactions to seven different addresses at WhiteBIT, as described below. Of the 4,890 SOL, approximately 2,211 SOL was sent in two transactions of approximately 1,500 SOL and approximately 710.753138909 SOL from “**DrkSpv...RQom**” to WhiteBIT. Approximately 1,500 SOL was sent to WhiteBIT deposit address “**JDZvMk...SB1K7**,” and approximately 710.753138909 SOL was sent to WhiteBIT deposit address “**EJe7Ca...Pb6nf**.”

36. On or about May 7, 2024, WhiteBIT's Anti-Money Laundering and Financial Monitoring Departments suspended 2,204.8222 SOL⁶ associated with the 1,500 SOL and 710.753138909 SOL deposits and thereafter consolidated that SOL into WhiteBIT address **8mowmVCEewZ9W2cEaQyQeQEeSxhGr1hvRviLwozwNtBt** (the Defendant Property).

37. North Korean cyber actors typically launder stolen funds through several exchanges, swapping currencies or value to different blockchains, to make following those assets more difficult and to prevent stolen funds from being frozen by law enforcement. What happened here is no different; the Lazarus Group, APT38, transferred the virtual currency to WhiteBIT to launder the virtual currency and obfuscate the nature, source, location, ownership, or control of stolen funds.

COUNT ONE – FORFEITURE OF DEFENDANT PROPERTY

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

38. Paragraphs 1 through 37 are realleged and incorporated by reference herein.

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

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

⁶ The difference between the 2,211 SOL that was deposited into those two WhiteBIT deposit addresses and the 2,204.8222 SOL that was frozen results from WhiteBIT's fee that was deducted during the transactions.

COUNT TWO – FORFEITURE OF DEFENDANT PROPERTY

(18 U.S.C. § 982(a)(1) and 18 U.S.C. § 981(a)(1)(A))

41. Paragraphs 1 through 37 are realleged and incorporated by reference herein.

42. The Defendant Property 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, computer fraud, wire fraud, and conspiracy to commit wire fraud and computer 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.

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

PRAYER FOR RELIEF

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

December 3, 2024
Washington, D.C.

Respectfully submitted,

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

/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.

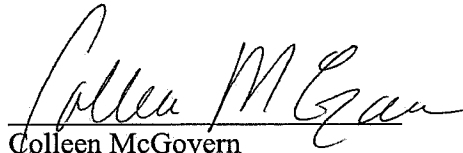
Gregory Jon Nicosia, Jr.
D.C. Bar No. 1033923
Trial Attorney, National Security Cyber Section
National Security Division
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530
Telephone: 202-353-4273
Email: Gregory.Nicosia@usdoj.gov

/s/ Rick Blaylock, Jr.

Rick Blaylock, Jr.
TX Bar No. 24103294
Assistant United States Attorney
Asset Forfeiture Coordinator
United States Attorney's Office
601 D Street, N.W.
Washington, D.C. 20001
(202) 252-6765

VERIFICATION

I, Colleen McGovern, 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.

A handwritten signature in cursive script, appearing to read "Colleen McGovern", is written over a horizontal line.

Colleen McGovern
Special Agent
Federal Bureau of Investigation