

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA**

<b>UNITED STATES OF AMERICA,</b>	)	
	)	
<b>Plaintiff,</b>	)	
	)	
<b>v.</b>	)	
	)	<b>Civil Action No. 24-cv-3309</b>
<b>ALL VIRTUAL CURRENCY SEIZED FROM</b>	)	
<b>ONE MEXC ACCOUNT ENDING IN 8248,</b>	)	
<b>ONE MEXC ACCOUNT ENDING IN 7017,</b>	)	
<b>ONE BINANCE ACCOUNT ENDING IN 8327,</b>	)	
<b>AND ONE BINANCE ACCOUNT ENDING IN</b>	)	
<b>5604.</b>	)	
<b>Defendants <i>in rem</i>.</b>	)	

**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 all currency seized from two MEXC and two Binance accounts, 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 Property involved in, and constituting the proceeds of, violations of wire fraud, wire fraud

conspiracy, money laundering, money laundering conspiracy, and computer fraud and abuse 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 virtual currency, seized from four accounts controlled by members of North Korean<sup>1</sup> military hacking groups known within the cybersecurity community as both the Lazarus Group, Advanced Persistent Threat (“APT38”)<sup>38</sup>, and CryptoMimic:

<u>Defendant Property</u>	<u>Account</u>	<u>Virtual Currency</u>	<u>Approx. Quantity</u>	<u>Approx. Value<sup>2</sup></u>
1	MEXC Account x8248	Bitcoin (BTC)	12	\$1,064,489.29
		Ether (ETH)	111	\$341,756.79
2	MEXC Account x7017	Tether (USDT)	48,692	\$48,721.22
		Ether (ETH)	145	\$446,439.05
		NFPrompt	1,289,329	\$328,907.83
3	Binance Account x8327	Tether (USDT)	90,915	\$90,969.55
4	Binance Account x5604	Bitcoin (BTC)	8	\$706,920.00
		Tether (USDT)	314,188	\$314,376.51

14. The Defendant Property 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 virtual currency hacks perpetrated by members of North Korean military hacking groups known within the cybersecurity community as the Lazarus Group,

<sup>1</sup> The Democratic People’s Republic of Korea is also known as “North Korea.”

<sup>2</sup> Values calculated on November 15, 2024.

APT38,<sup>3</sup> and CryptoMimic. These nefarious actors use distinctive tactics, techniques, and procedures observed in other 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. Since at least late 2014, the subjects have also targeted banks and virtual currency exchanges and have successfully initiated fraudulent transfers at both. 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.

16. 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 federal and foreign law enforcement agencies; and most importantly: to recover assets that may be used to compensate victims.<sup>4</sup>

### **Background Regarding the CryptoMimic Investigation**

17. As part of its investigation of the group referred as CryptoMimic, also known as

---

<sup>3</sup> APT 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, APT38.

<sup>4</sup> See United States Asset Forfeiture Program, *Our Mission*, <https://www.justice.gov/afp>.

APT38 and Lazarus Group, the FBI proactively identified servers located in the United States and abroad that perform command-and-control (“C2”) functions for malware used by CryptoMimic (the “CryptoMimic C2 Servers”). These CryptoMimic C2 Servers act as points of interface between the North Korean cyber actors controlling them and the victim computers that are compromised with their malware.

18. Between approximately October and December 2023, the FBI identified and interviewed several individuals employed by virtual asset service providers whose computers were compromised with malware in circumstances involving a common pattern. In short, North Korean cyber actors created numerous fake online personas imitating personnel at venture capital firms who were well known for investing in virtual currency companies. One of these fake personas was named after CEO-1, using the real name of the Chief Executive Officer (CEO) of COMPANY-1, a Hong Kong-based venture capital firm prominent in the virtual currency industry. These fake North Korean personas contacted executives at various virtual currency firms and invited them to a video conference to discuss potential investments in their companies. The North Korean imposters sent links to targeted executives purportedly to join the video conference, but the links directed victims to web pages which displayed an error message. The personas would offer to help the victims troubleshoot the error, then send them a file of computer code called a “script,” allegedly to fix the problem. However, these scripts contained code that instead downloaded malware from one of the CryptoMimic C2 Servers to the victim computer; that malware then began communicating with one or more of the CryptoMimic C2 servers.

19. Pursuant to court-authorized legal process, the FBI obtained data which shows some instances in which CryptoMimic actors connected to some CryptoMimic C2 Servers. Although in most of these instances, the CryptoMimic actors connected to their C2 Servers via virtual private

network (VPN) services,<sup>5</sup> some connections were directly from IP addresses located in North Korea. For example, two particular CryptoMimic C2 Servers were accessed by cyber actors located in North Korea. One North Korean IP address, 175.45.178.[x]<sup>6</sup>, repeatedly accessed “C2 Server 1” between on or about January 24, 2024, and on or about March 15, 2024. Another North Korean IP address repeatedly accessed “C2 Server 2” between on or about November 28, 2023, and on or about March 15, 2024.

### **Background Regarding the COMPANY-2 Theft**

20. On or about March 13, 2024, U.S.-based representatives of the online platform COMPANY-2 filed a complaint with the FBI stating that they had been the victim of a theft of approximately \$34 million in virtual currency.

21. On or about March 14, 2024, FBI agents interviewed a COMPANY-2 employee. That employee stated, in sum and substance, that in or around November 2023, while the employee was traveling in China to meet with the CEO of COMPANY-2, the CEO was in communication with an individual who claimed to be CEO-1, the prominent venture capitalist referenced above, via Telegram, a digital messaging service that offers end-to-end encryption. During these

---

<sup>5</sup> A VPN creates a secure, encrypted connection, or tunnel, between the end user (i.e., the customer of the VPN service) and a server operated by the VPN service. Thus, when an end user wants to visit a particular website, the end user’s internet traffic is routed first to a VPN server through an encrypted connection before the VPN server connects with that website. A VPN provides the benefit of encrypting the data between the end user and VPN server so that the data cannot be eavesdropped on by (1) other users on the same Wi-Fi network, (2) the user’s internet service provider (or “ISP”), or (3) other routers or devices between the user and the VPN server. Many VPN providers also provide the option for the end user to select a VPN server in a specific geographic region to which he or she will connect, which allows the user to appear to the websites visited as though the end user is in that geographic region. VPNs are thus one way that a cybercriminal may hide his or her identity or location.

<sup>6</sup> The final segment, or “octet,” of this IP address has been redacted. However, all IP addresses beginning with 175.45.178 are assigned to North Korea.

communications, the COMPANY-2 CEO clicked on a link to join a video conference with the individual purporting to be CEO-1, but the link did not seem to work. The imposter then sent the COMPANY-2 CEO a script file to fix the problem, which the COMPANY-2 CEO executed on the employee's computer.

22. During the interview, the employee further stated that part of the funds stolen from COMPANY-2 were in the form of cryptocurrency native to COMPANY-2's platform. According to the employee, the employee stored a text file on their computer containing the private keys for approximately 5,000 addresses holding COMPANY-2's native token. The perpetrators seemingly deleted this file from the employee's computer, eliminating access by COMPANY-2.

23. Based on analysis of data the FBI received from the employee and from court-authorized legal process, the COMPANY-2 employee's computer likely connected to C2 Server 1 and C2 Server 2 at least 18 times between approximately March 11, 2024, and March 13, 2024.

24. These facts are consistent with the CryptoMimic impersonations described above. In other words, the evidence indicates that CryptoMimic actors were behind this deployment of malware, and that it resulted in the theft of funds from COMPANY-2.

### **Tracing the Stolen COMPANY-2 Funds**

25. During the heist, North Korean cyber actors stole several virtual currencies, including NFP. They stole approximately 19 million NFP, valued at the time of the heist at approximately \$17 million, from a total of approximately 2,600 separate virtual currency addresses. The NFP were transferred from the approximately 2,600 addresses to one address, 0x60275d1cC368CF021547a82a51cFb8C055390DA3 ("0x60275d"). In other words, the funds were consolidated into that 0x60275d address. After consolidation, the perpetrators sent NFP in a series of transfers from 0x60275d to several other virtual currency addresses, as outlined below:



a. Two transfers, totaling 1,500,000 NFP, were sent to 0xa465480BF622e835ceE55620e7ae5870d02ecbFa, a MEXC deposit address. Per records provided by MEXC, this was associated with **Defendant Property 1**, which is a MEXC account with UID ending in 8248.

b. Six transfers, totaling 3,600,100 NFP, were sent to 0xb98C2390ce8a05FbFE221dC9bc2B911a9Ca2a2De, a MEXC deposit address. Per records provided by MEXC, this was associated with **Defendant Property 2**, which is a MEXC account with UID ending in 7017.

c. One transfer, totaling 100,000 NFP, sent to 0xe6e8521871D0e3c21B09E12012D33407891DB169, a Binance deposit address. Per records provided by Binance, this address was associated with **Defendant Property 3**, which is a Binance account with User ID (UID) ending in 8327.

d. Two transfers, totaling 1,000,100 NFP, were sent to 0x342ed3d121010C725FAF6d3446c1931EBFcE8398, a Binance deposit address. Per records provided by Binance, this was associated with **Defendant Property 4**, which is a Binance account with UID 5604.

26. MEXC voluntarily froze **Defendant Properties 1 and 2**, and Binance voluntarily frozen **Defendant Properties 3 and 4**.

27. MEXC account with UID x8248, that is, the account containing **Defendant Property 1**, was created on or about March 14, 2024. The only deposits to the account were the two transfers of NFP described above, the first of which was made approximately eleven minutes after the account was created. Prior to being frozen, the account executed nearly 1,300 trades to convert all of the NFP to USDT, BTC, and ETH. The value remaining in the account was approximately 0.07 USDT, 12

BTC, and 111 ETH, which was equivalent to approximately \$1,245,000 at the time of seizure.

28. MEXC account with UID x7017, that is, the account containing **Defendant Property 2**, was created on or about March 14, 2024. The only deposits to the account were the six transfers of NFP described above, the first of which was made approximately four minutes after the account was created. Prior to being frozen, the account executed over 5,600 trades to convert much of the NFP to ether (ETH), which is the native virtual currency on the Ethereum network, and USDT, a stablecoin pegged to the U.S. dollar. On or about March 14, 2024, approximately 356 ETH was withdrawn from the account. The value remaining in the account was approximately 48,706 USDT, 145 ETH, and 1,289,329 NFP, which was equivalent to approximately \$1,679,000 as of the time of seizure.

29. Binance subsequently provided records that showed the Binance account with UID x8327, that is, the account containing **Defendant Property 3**, was created on or about December 10, 2023. As described above, on or about March 13, 2024, one transfer of 100,000 NFP was sent to the account containing **Defendant Property 3**. Prior to the freeze, this account executed two trades to convert all 100,000 NFP to a total of 91,313 USDT. The value remaining in the account was approximately 90,915 USDT, which was equivalent to approximately \$90,915 as of the time of seizure.<sup>7</sup>

30. Binance account with UID x5604, that is, the account containing **Defendant Property 4**, was created on or about January 5, 2023. Prior to the March 13, 2024, heist, the account received one deposit of 128 USDT. Prior to being frozen, the account containing **Defendant**

---

<sup>7</sup> Although not clearly specified in records provided by Binance, it appears as though Binance charged transaction fees to perform trades for Defendant Properties 3 and 4, as the balances are slightly less than the traded funds with no indication of withdrawals from the accounts.

**Property 4** executed eight trades to convert all 1,000,100 NFP to approximately 340,727 USDT and approximately 8 BTC, then subsequently withdrew approximately 90 USDT. The value remaining in the account was approximately 314,188 USDT and 8 BTC, which was equivalent to approximately \$844,000 as of the time of seizure.

**COUNT ONE – FORFEITURE OF DEFENDANT PROPERTY**

**18 U.S.C. § 981(a)(1)(C)**

31. Paragraphs 1 through 30 are realleged and incorporated by reference here.

32. The Defendant Property 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.

33. Accordingly, the Defendant Property 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)**

34. Paragraphs 1 through 30 are realleged and incorporated by reference here.

35. 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, wire fraud, conspiracy to commit wire fraud, computer fraud and abuse, and conspiracy to commit computer fraud and abuse 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.

36. Accordingly, the Defendant Property 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.

November 21, 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, 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 21<sup>st</sup> day of November, 2024.

  
\_\_\_\_\_  
Justin M. Vallese  
Special Agent  
Federal Bureau of Investigation