

IN THE UNITED STATES DISTRICT COURT  
DISTRICT OF KANSAS

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Case No. <u>22-1154</u>
	)	
Defendant No. 1:	)	
Contents of account with User ID	)	
XXXX5190 seized on or about	)	
May 5, 2022,	)	
	)	
Defendant No.2:	)	
Contents of account with User ID	)	
XXXX7082 seized on or about	)	
May 5, 2022.	)	
	)	
Defendants.	)	

**COMPLAINT FOR FORFEITURE IN REM**

Plaintiff, United States of America, by and through its attorneys, Duston J. Slinkard, United States Attorney for the District of Kansas, and Annette Gurney, Assistant United States Attorney, brings this complaint and alleges as follows in accordance with Supplemental Rule G(2) of the Federal Rules of Civil Procedure:

**NATURE OF THE ACTION**

1. This is an *in rem* action to forfeit and condemn to the use and benefit of the United States of America, the above-captioned defendants for violations of 18 U.S.C. §§ 371, 1030, 1956(a)(1)(B)(i) and 1956(h).

**THE DEFENDANTS IN REM**

2. The defendants are the contents of two virtual currency accounts that were seized from a virtual currency exchange by the Federal Bureau of Investigation (FBI) on or about May

5, 2022. The defendants are currently in the custody of the FBI.

### **JURISDICTION AND VENUE**

3. Plaintiff brings this action *in rem* in its own right to forfeit and condemn the defendants pursuant to 18 U.S.C. §§ 981(a)(1)(A) and (C).

4. This Court has jurisdiction over an action commenced by the United States under 28 U.S.C. §1345, and over an action for forfeiture under 28 U.S.C. §1355(a).

5. Venue is proper in this district pursuant to 28 U.S.C. § 1355(b)(1), because acts or omissions giving rise to the forfeiture of the defendants occurred in this district.

### **BASIS FOR FORFEITURE**

6. The defendants are subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A) because they constitute property involved in a transaction or attempted transaction in violation of 18 U.S.C. §§ 1956 (a)(1)(B)(i) and 1956 (h). The defendants are also subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C) because they constitute or are derived from proceeds traceable to violations of 18 U.S.C. §§ 371 and 1030.

7. Supplemental Rule G(2)(f) requires this complaint to state sufficiently detailed facts to support a reasonable belief that the government will be able to meet its burden of proof at trial. Such facts and circumstances supporting the seizure and forfeiture of the defendants are contained in Exhibit A which is attached hereto and incorporated by reference.

8. As a result of the foregoing, the defendants are liable to condemnation and forfeiture to the United States for its use, in accordance with 18 U.S.C. § 981.

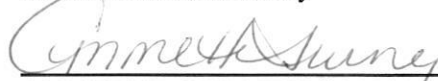
**CLAIM FOR RELIEF**

WHEREFORE, the United States prays that the Court issue a warrant for the arrest *in rem* of Defendants No. 1 and 2; that notice of this action be given to all persons who reasonably appear to be potential claimants of interests in the defendants; that the defendants be forfeited and condemned to the United States of America; that the plaintiff be awarded its costs and disbursements in this action; and for such other and further relief as this Court deems proper and just.

The United States hereby requests that trial of the above-entitled matter be held in the City of Wichita, Kansas.

Respectfully submitted,

Duston J. Slinkard  
United States Attorney

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

ANNETTE GURNEY #11602  
Assistant United States Attorney  
1200 Epic Center, 301 N. Main  
Wichita, Kansas 67202  
(316) 269-6481 FAX: (316) 269-6684  
annette.gurney.usdoj.gov


**DECLARATION**

I, Kelly G. Sallee, am a Special Agent with the Federal Bureau of Investigation (FBI).

I have read the contents of the foregoing Complaint for Forfeiture and the exhibits thereto, and the statements contained therein are true to the best of my knowledge and belief.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on this 18<sup>th</sup> day of July, 2022.

  
\_\_\_\_\_  
Kelly G. Sallee  
Special Agent  
FBI

**AFFIDAVIT IN SUPPORT OF COMPLAINT FOR FORFEITURE**

I, Kelly G. Sallee, being duly sworn, depose and state as follows:

**I. INTRODUCTION**

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since September 7, 2003. I am currently assigned to the FBI Kansas City Division's Cyber Crimes Task Force. As a Special Agent with the FBI, I investigate criminal and national security related computer intrusion matters involving botnets, malicious software, the theft of personal identification information, and other computer-based fraud. Since joining the FBI, I have been involved in several criminal and national security investigations involving computer intrusions and virtual currencies. I have received FBI training in computer technology and computer-based fraud. I am also a Certified Public Accountant and a Certified Fraud Examiner and have attended yearly Continuing Professional Education for those certifications that involved training for virtual currencies.

2. This affidavit is in support of a complaint for forfeiture against the following property:

A. Contents of account with User ID XXXX5190 ("VCE Account A"), seized from a virtual currency exchange on or about May 5, 2022.

B. Contents of account with User ID XXXX7082 ("VCE Account B"), seized from a virtual currency exchange on or about May 5, 2022.

3. The investigation detailed herein is being conducted by the FBI Kansas City Division's Cyber Crimes Task Force. The facts set forth herein are intended to show that there is probable cause to believe that the two virtual currency accounts described in paragraph 2 contain proceeds of a computer intrusion conspiracy committed in violation of 18 U.S.C. §§ 371 and 1030, and constitute property involved in a money laundering conspiracy in violation of 18 U.S.C. §§ 1956(a)(1)(B)(i) and 1956(h).



## **II. BACKGROUND REGARDING VIRTUAL CURRENCY**

4. Virtual currencies are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency.

5. Virtual currency addresses are the digital 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.

6. Virtual currency exchanges are online trading and/or storage platforms for virtual currencies, such as Bitcoin (BTC). These exchanges store their customers' virtual currency in online virtual currency accounts.

7. Some virtual currencies, including BTC, publicly record all their transactions on what is known as a blockchain. The blockchain is a permanent public ledger containing a historical record of every transaction utilizing that blockchain's technology. The blockchain records every virtual currency address that has ever received that virtual currency and can be used to calculate balances for each virtual currency address. There are different blockchains for different types of virtual currencies.

8. Blockchain explorers are online tools that operate as a blockchain search engine allowing users the ability to search for and review transactional data for any address on a particular blockchain. The blockchain explorer uses a database to arrange and present the data to a user in a searchable format.

9. Law enforcement can sometimes identify information about the owner of a particular virtual currency address by analyzing the blockchain (e.g., the BTC blockchain). The analysis can also reveal additional addresses controlled by the same individual or entity.

### **III. OVERVIEW OF THE COMPUTER INTRUSION**

#### **A. Ransomware Attack on Kansas Medical Provider**

10. Officials working on behalf of a medical provider located in the District of Kansas advised the FBI that on or around May 4, 2021, the provider became the victim of a ransomware attack. On May 4, 2021, the Kansas medical provider's employees discovered they could not access files. Instead, attempts to open files resulted in receipt of an error message stating that the file format had changed.

11. The Kansas medical provider's employees were unable to access the PACS server, which is used for x-rays and diagnostic imaging; the EDM server, which is used for scanning data; the internet server; and the sleep lab server.

12. The Kansas medical provider's information technology team assessed the impact of the incident and determined that at least these four physical servers had been encrypted using ransomware. Based on my training and experience, I know that ransomware is a type of malware that is designed to block access to a computer system until a ransom is paid, generally through virtual currency. The Kansas medical provider and the FBI determined that the malware software was named "maui.exe".

13. The Kansas medical provider's team found a ransom note on one of the affected systems. The ransom note stated that payment would need to be made to have the files restored. The note demanded a payment of 2.0 BTC be sent to an address herein referred to as "Ransomware BTC Address No. 1." If payment was not made in forty-eight hours, the note stated that the price would double.

14. The FBI has confirmed that on May 11, 2021, a payment for 1.66 BTC was made on the Kansas medical provider's behalf to Ransomware BTC Address No. 1.

15. The FBI has confirmed that on May 17, 2021, a payment for 0.11 BTC was made on the Kansas medical provider's behalf to the same BTC address, Ransomware BTC Address No. 1. The ransomware co-conspirators subsequently provided the Kansas medical provider the decryption keys to decrypt and access their systems and files.

16. I have probable cause to believe that the 1.77 BTC (which at the time of transfer was worth approximately \$100,000) that the Kansas medical provider paid to Ransomware BTC Address No. 1 constitutes proceeds of a computer intrusion committed in violation of 18 U.S.C. §§ 371 and 1030.

17. As part of its investigation, the FBI determined that the maui.exe software was a previously unseen form of malware, meaning that it had not previously been reported to law enforcement. On July 6, 2022, the FBI, the Cybersecurity and Infrastructure Security Agency, and the Department of Treasury announced that the maui.exe ransomware was being used by North Korean state-sponsored cyber actors to target healthcare organizations. The announcement stated that because those organizations provide services critical to human life and health, they are more willing to pay ransoms.

18. On August 12, 2021, as part of the investigation into the users of the maui.exe ransomware, the FBI obtained records from a virtual currency exchange for the virtual currency exchange's customer accounts which the BTC blockchain showed had received deposits from Ransomware BTC Address No. 1 (the address where the Kansas medical provider sent the 1.66 BTC and 0.11 BTC ransom payments on May 11 and 17, 2021).

19. According to the virtual currency exchange's records, on May 12, 2021, a 1.66 BTC transfer from Ransomware BTC Address No. 1 was sent to a BTC address associated with VCE Account A.



20. According to the virtual currency exchange's customer records, VCE Account A belongs to user ID XXXX5190.

21. Based on my training and experience, I know that ransomware actors will sometimes move virtual currency funds from the virtual currency address listed in the ransom note to conceal their possession and use of those funds. I, therefore, have probable cause to believe that the financial transaction involving the movement of the BTC from Ransomware BTC Address No. 1 to VCE Account A, which contained proceeds from the computer intrusion against the Kansas medical provider, constitutes a violation of 18 U.S.C. §§ 1956 (a)(1)(B)(i) and 1956(h).

22. The FBI also obtained records from the virtual currency exchange, which showed that on June 25, 2021, a 0.21 BTC transfer from Ransomware BTC Address No.1 was sent to a BTC deposit address associated with VCE Account B.

23. According to the virtual currency exchange's customer records, VCE Account B belongs to user ID XXXX7082.

24. Based on my training and experience, I have probable cause to believe that the financial transaction involving the movement of the BTC from Ransomware BTC address Address No. 1 to VCE Account B, which contained proceeds from the computer intrusion against the Kansas medical provider, constitutes a violation of 18 U.S.C. §§ 1956 (a)(1)(B)(i) and 1956(h).

25. The virtual currency exchange's records further revealed that VCE Accounts A and B had frequently logged in from the same Hong Kong-based IP address, providing further evidence (besides the tracing of the ransomware payments) that the two accounts are connected to one another.

**B. Ransomware Attack on Colorado Medical Provider**

26. The FBI's investigation revealed that on April 1, 2022, VCF Account B received an additional 1.32 BTC from a U.S.-based virtual currency exchange.

27. By tracing the April 1 payment into VCE Account B back to its source, the FBI's investigation revealed that another U.S.-based medical provider, this time located in Colorado, was hacked and its files were encrypted using the maui.exe software. Specifically, an incident response company confirmed to the FBI that, on March 30, 2022, the company made a payment of 2.54 BTC on behalf of the Colorado medical provider to a BTC address provided by the hacker: "Ransomware BTC Address 2." Based on my training and experience, this 2.54 BTC (which at the time of transfer was worth approximately \$120,000) constitutes proceeds of a computer intrusion conspiracy committed in violation of 18 U.S.C. §§ 371 and 1030.

28. According to the blockchain analysis and records received from the virtual currency exchange, this 2.54 BTC was moved the same day (March 30, 2022) from Ransomware BTC Address No. 2 to "Ransomware BTC Address No. 3. Then on April 1, 2022, the above-referenced 1.32 of this 2.54 BTC was moved from Ransomware BTC Address 3 to VCE Account B.

29. Because the maui.exe software is new and relatively rare, and because the ransom payment was also deposited into VCE Account B, there is probable cause to believe that the Colorado medical provider was a victim of the same ransomware conspiracy that had victimized the Kansas medical provider.

30. Based on my training and experience, there is probable cause to believe that the financial transaction involving the movement of the 1.32 BTC from Ransomware BTC Address

No. 3 to VCE Account B, which contained proceeds of the computer intrusion against the Colorado medical provider, constitutes a violation of 18 U.S.C. §§ 1956(a)(1)(B)(i) and 1956(h).

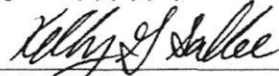
31. On or about May 5, 2022, VCE Account A was seized pursuant to a seizure warrant issued out of the District of Kansas.

32. On or about May 5, 2022, VCE Account B was seized pursuant to a seizure warrant issued out of the District of Kansas.

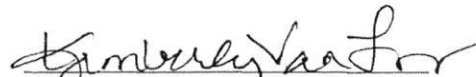
#### IV. CONCLUSION

33. Based upon the foregoing, probable cause exists to believe that the contents of VCE Accounts A and B identified in paragraph 2 contain proceeds traceable to a computer intrusion conspiracy committed in violation of 18 U.S.C. §§ 371 and 1030 against U.S. medical providers. Based on these crimes, the seized virtual currency is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C).

34. Additionally, based upon the foregoing, probable cause exists to believe that the contents of the VCE Accounts A and B identified in paragraph 2 constitute property involved in transactions in violation of 18 U.S.C. §§ 1956(a)(1)(B)(i) and 1956(h), and, therefore, the seized virtual currency is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A).

  
\_\_\_\_\_  
Kelly G. Sallee  
Special Agent  
Federal Bureau of Investigation

Sworn before me this 15 day of July, 2022.

  
\_\_\_\_\_  
Notary Public

My commission expires 10/6/2023

