IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS

IN THE MATTER OF THE SEIZURE OF ENTIRE CONTENTS OF PAXFUL USER ID ACCOUNT 4690943, LOCATED AT PAXFUL, INC., A VIRTUAL CURRENCY EXCHANGE	Case No. 24-mj-08113-ADM ~~**Filed Under Seal**~~

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEIZURE WARRANTS

I, [redacted], 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 October 2023. I have been assigned to the St. Louis Field Office. I am currently assigned to conduct investigations related to criminal and national security computer intrusion and virtual currency matters. During my law enforcement career, I have conducted and participated in numerous computer crime investigations. In addition, I have received both formal and informal training from the FBI and other organizations regarding investigation techniques, computer technology, and cybercrime tactics.

2. This investigation is being conducted by the FBI Kansas City Division's Cyber Crimes Task Force and the FBI St. Louis Division. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses, including an FBI forensic accountant. Because this affidavit is being submitted for the limited purpose of establishing probable cause in support of an application for the seizure warrants described herein, it does not set forth each and every fact that I or others have learned during the course of the investigation.

II. PROPERTY TO BE SEIZED

3. This affidavit is being submitted in support of an application for a civil seizure warrant for the contents of the account listed in Attachment A-1 to this Affidavit ("**Subject Account 1**"), which

is held by Binance Holdings Limited ("Binance"), and the contents of the account listed in Attachment A-2 to this Affidavit ("**Subject Account 2**"), which is held by Paxful, Inc. ("Paxful"). Binance and Paxful are online exchanges that offer accounts for customers to store and trade virtual currency.

4. Based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel, the facts as set forth in this affidavit are intended to show that there is probable cause to believe that **Subject Account 1** and **Subject Account 2**, described in Attachments A-1 and A-2, contain property involved in a transaction or attempted transaction in violation of 18 U.S.C. §§ 1956(a)(1)(B)(i) (concealment money laundering) and 1956(h) (conspiracy to commit money laundering), or any property traceable to such property.

III. BACKGROUND REGARDING VIRTUAL CURRENCY

5. Virtual currencies are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Virtual currencies are 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. Bitcoin (or BTC) is currently one of the most popular virtual currencies in use. Other common virtual currencies include Ether (or ETH) and Tether (or USDT).

6. 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.

7. Virtual currency exchanges, like Paxful and Binance, are trading and/or storage platforms for virtual currencies, such as BTC. Many exchanges also store their customers' virtual currency in virtual currency accounts. These virtual currency accounts are commonly referred to as wallets and can hold multiple virtual currency addresses.

8. Many virtual currencies, including BTC, publicly record all their transactions on what is known as a blockchain. The blockchain is a distributed public ledger 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.

9. 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 addresses on a particular blockchain. The blockchain explorer uses a database to arrange and present the data to a user in a searchable format.

10. 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).

11. Over the course of this investigation, the FBI conducted detailed blockchain analysis. 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 relationships between transactions, wallets, and accounts in a manner that allows for them to be linked to groups or individuals (although the exact identity of the underlying individuals is not available on the blockchain). Through

numerous unrelated investigations, law enforcement has found the information provided by these companies to be reliable.

IV. OVERVIEW OF THE ANDARIEL COMPUTER INTRUSIONS, MONEY LAUNDERING CONSPIRACY, AND PREVIOUS SEIZURES

12. This investigation began when officials working on behalf of a Kansas Medical Provider advised the FBI that on or around May 4, 2021, the Kansas Medical Provider became the victim of a ransomware attack. On that date, the Kansas Medical Provider employees discovered that they could not access some of their electronic files. Instead, attempts to open files resulted in receipt of an error message stating that the file format changed.

13. The Kansas Medical Provider employees were unable to access the PACS server, used for x-rays and diagnostic imaging; the EDM server, used for scanning data; the intranet server; and the sleep lab server.

14. 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. The Kansas Medical Provider determined that the malware executable file was named "maui.exe." Ransomware is a type of malware that is designed to block access to a computer system until a ransom is paid, often through virtual currency.

15. The Kansas Medical Provider's team found a ransom note on one of the affected systems. The ransom note stated that a virtual currency payment would need to be made to have the files restored. If no payment was made, the files would be posted on the internet.

16. The FBI's investigation confirmed that on May 11, 2021, a payment for 1.66 BTC was made on the Kansas Medical Provider's behalf to a BTC address controlled by the ransomware actor. The FBI also confirmed that on May 17, 2021, an additional payment for 0.11 BTC was made on the Kansas

Medical Provider's behalf to the same BTC address. The ransomware actors subsequently provided the Kansas Medical Provider the decryption keys to decrypt and access their systems and files.

17. The Kansas City FBI Cyber Crimes Task Force opened an investigation into the computer intrusion and ransomware attack upon the Kansas Medical Provider.

18. As part of the investigation, the FBI determined that the maui.exe software was a previously unseen form of malware, indicating that the attack was not part of a known variant and not previously reported to law enforcement. The FBI identified email and other online accounts used by the malicious cyber actors, reviewed the maui.exe malware, and traced bitcoin ransom payments through different addresses. By doing this, the FBI identified additional victims of the conspiracy and obtained information indicating that the malicious actors were state-sponsored North Korean ("DPRK") hackers. *See* Joint Cybersecurity Advisory, *North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector* (July 6, 2022), *available at* https://www.cisa.gov/sites/default/files/publications/aa22-187a-north-korean%20state-sponsored-cyber-actors-use-maui-ransomware-to-target-the-hph-sector.pdf.

19. The FBI previously seized nearly $500,000 in cryptocurrency related to Maui ransomware victims from two Binance accounts. *See* Case No. 2:22-mj-08087-ADM (seizure warrant signed May 5, 2022).

V. PROBABLE CAUSE FOR SEIZURE OF SUBJECT ACCOUNTS

A March 2023 Ransomware Attack on a South Korean Manufacturing Company Was Part of the Conspiracy

20. In late March of 2023, South Korean Manufacturing Company was the victim of a ransomware attack. Attackers stated that they deployed "zombie" ransomware, and South Korean Manufacturing Company negotiated a ransom with the user of email address tayronqxhardy07[@]gmail.com. The FBI linked this attack to the North Korean co-conspirators behind

Maui ransomware attacks, including the attack at the Kansas Medical Provider, and other computer intrusions. Security researchers refer to this group publicly as Andariel, among other names.

21. Email address tayronqxhardy07[@]gmail.com has been linked to the DPRK-based Andariel co-conspirators in multiple ways. First, the same IP address that accessed other Andariel-linked Google accounts also accessed tayronqxhardy07[@]gmail.com. That IP address also accessed a Dropbox account that was used to store exfiltrated data from other Andariel victims. Second, a known Andariel account was used as the recovery address for tayronqxhardy07[@]gmail.com. The user of that recovery address registered a domain at an IP address used to conduct an Andariel Maui ransomware attack on a Florida hospital in March 2022. The government previously obtained a search warrant for tayronqxhardy07[@]gmail.com, which also showed it was linked by cookie[1] to numerous other Andariel-controlled Google accounts.

22. After negotiations, the hacker controlling tayronqxhardy07[@]gmail.com provided bitcoin address bc1q9zhkxl7nm2jmfee3xnvm73n2g9fxaszvj0q79r ("the bc1q9zh address")[2] to South Korean Manufacturing Company. The FBI confirmed that on April 12, 2023, a ransom payment of 4.29 BTC[3] (approximately $130,000) was made on behalf of the victim to the bc1q9zh address.

Tracing the Ransom Proceeds from the bc1q9zh Address: December 2023 Activity

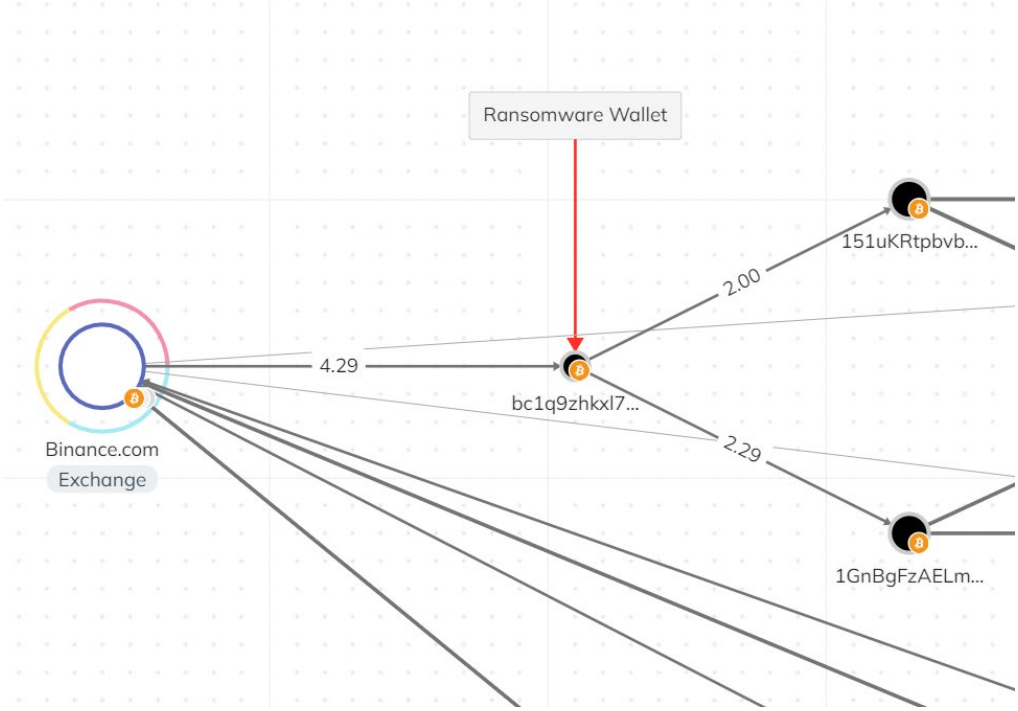
23. The ransom funds sat in the bc1q9zh address from April 12, 2023, until December 13, 2023, without moving. On December 13, 2023, the ransom funds were transferred from the bc1q9zh

[1] A "cookie" is a small file containing a string of characters that email providers, including Google, place onto a user's computer or device. When that computer visits again, the website will recognize the cookie and identify the same user who visited before. This sort of technology can be used to track users across multiple websites and online services belonging to providers like Google. From my training and experience, I know that cookies and similar technology used by providers such as Google may constitute evidence of the criminal activity under investigation. By linking various accounts, devices, and online activity to the same user or users, cookies and linked information can help identify who was using a Google account and determine the scope of the criminal activity.

[2] Throughout this affidavit, after including a complete cryptocurrency address, I will then refer to it by referencing the first seven characters of the address.

[3] Unless otherwise stated, cryptocurrency amounts in this affidavit are approximations.

address to two separate addresses. First, at approximately 12:58 a.m. UTC, the bc1q9zh address sent 2 BTC to 151uKRtpbvb8d7yQRpKgdomoiHFAAWs756. Then, at approximately 1:56 a.m. UTC, the bc1q9zh address sent the remaining 2.29 BTC to 1GnBgFzAELmgsujWXNEnm22uYnHw981RnX. This is depicted in the following graph:



24. Between December 13 to December 15, 2023, the ransom funds were transferred from the 151uKRt address and the 1GnBgFz address to two deposit addresses at MEXC, which I know from my training and experience to be a cryptocurrency exchange. The government obtained records from MEXC, which show that funds from the 151uKRt address were deposited into address 3JF1vVxH8ZoReNrmaRbQXrvgJyszQoEefN, associated with a particular MEXC account, and the funds from the 1GnBgFz address were deposited into address 3K5GR5XkeusbY28QfFWB9S6sDZJbgQZKT6, associated with a different MEXC account.

25. The MEXC account in control of the 3JF1vVx address received approximately 4.28 BTC between December 12 and December 14, 2023. During this time period, MEXC records show that the

account owner transferred approximately 66.8 ETH and approximately 29,030.73 USDT to another address: 0xfC37D6810e724B9D25e4eC720F972aa2d94ebe4F. The account had no other transaction history and no remaining balance.

26. Between December 12 and December 14, 2023, the 0xfC37D address transferred all its value to two other addresses, 0xF9ABFe05423E6BdEB6FF522D13C72a36fc2f345D and 0x63B0E131AA4483C3F55834325eFe493F35ca859a.

27. Between December 12 and December 14, 2023, the 0xF9ABF address transferred 45.05 ETH and 29,030 USDT to address 0x9E627bB47ca34f85eD05b6d7978b70E5C2D21Ce6, which is controlled by a MEXC accountholder. The 0xF9ABF address also transferred 13.153 ETH to the 0x63B0E address on December 13, 2023.

28. MEXC records indicate that the MEXC account in control of the 3K5GR5X address, which received ransom funds as described in paragraph 24, received 2.29 BTC from December 13 to December 15, 2023, and transferred 42.87 ETH to address 0x56bec0626608A2A3C05eC164FBB2a1554c9Ee5C3. The MEXC account had no remaining balance or other transaction history.

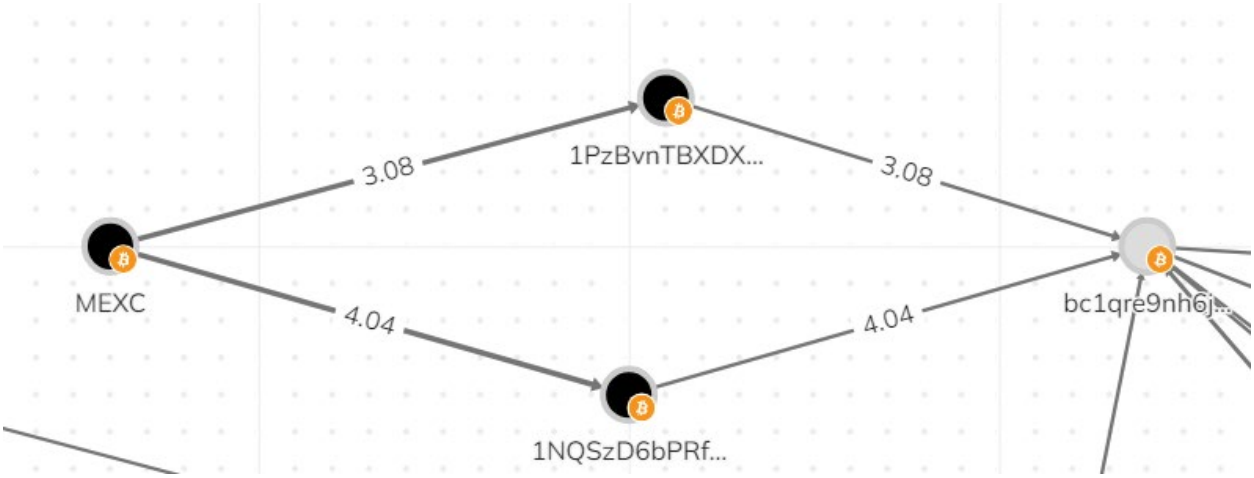
29. The 0x56bec address sent 42.87 ETH to the 0x63B0E address between December 13 and 15, 2023. During the same time period, the 0x63B0E address deposited 76.046 ETH into address 0xe3CC3AFFb10b83Bbc405aD9D0B7870E7b4E1E1F7, controlled by a MEXC account.

30. MEXC provided additional records. The 0x9E627 address, discussed in paragraph 27, is controlled by a MEXC account that received 45.05 ETH and 29,030.73 USDT between December 12 and 13, 2023. The MEXC account controlling the 0x9E627 address transferred 3.08 BTC to address 1PzBvnTBXDXhd5C5stnjaYnRKdyzDj8ENr during the same time period. As of December 27, 2023, the MEXC account had no other transactions and no remaining balance.

31. The 1PzBvnT address, which received the 3.08 BTC, transferred 3.079 BTC to bc1qre9nh6ju6rgzhq8zavz4xys8thdwy5z6tquytp on December 17, 2023.

32. MEXC provided records on another account, the account that controls the 0xe3CC3 address described in paragraph 29. This account transferred 4.042 BTC to address 1NQSzD6bPRfyqjgFANimyZRW7ruyq2xowU between December 13 and December 15. As of December 27, 2023, the MEXC account had no other transaction history other than that described in paragraph 29 and this paragraph, and no remaining balance.

33. On December 17, 2023, the 1NQSzD6 address, which received the 4.042 BTC, transferred 4.039 BTC to the bc1qre9 address discussed in paragraph 31, as displayed in the following graph:



Thus, after traveling from the South Korean ransomware victim through virtual currency addresses to two MEXC accounts, and then again through virtual currency addresses back to two other MEXC accounts, approximately 7.12 BTC was consolidated in the bc1qre9 address on the right of this graph. This 7.12 BTC stayed in the bc1qre9 address until April 17, 2024.

Tracing the Proceeds from the bc1qre9 Address to Subject Accounts 1 and 2: April 2024 Activity

34. On April 17, 2024, at approximately 4:07 UTC, actors transferred a total of approximately 3.079 BTC from the bc1qre9 address to two other addresses:

bc1qzcwludsf86xjecaypg5j62z56j5ruffzh3frfa (0.783 BTC) and bc1qqdr7ewh4pgy902ml5tnre2qq8mxqf7e9xs2pmd (2.296 BTC).

35. Subsequently, on April 17, 2024, the bc1qzcw address transferred all of its bitcoin to Paxful deposit address 32D4pk4nkiaY4NMpeJi47drz9cNCwdmbqw in two transactions, one with 0.392 BTC and another with 0.391 BTC.

36. On April 23, 2024, the bc1qqdr address transferred approximately 1.6 BTC to bc1qzq4mt2wedrc7jjtapjm9v3z6mx4pzeqqqgkn0w.

37. On April 23, 2024, the bc1qzq4 address transferred approximately 0.979 BTC to bc1qnhshvz4d4f6wn9kuk2s8q7p54zxmctwvdh7ghv.

38. On April 29, 2024, according to records provided by Binance, the bc1qnhs address transferred 0.45 BTC to the Binance deposit address 1KDVni5ocXL9gbAZXmjDHvaowAYZeaa8xE, distributed across three transactions.

39. This means that ransom funds flowed from the bc1qre9 address to the bc1qqdr address to the bc1qzq4 address to the bc1qnhs address, and ultimately to the 1KDVni5 address. The 1KDVni5 address, controlled by **Subject Account 1**, has received multiple deposits from the bc1qnhs address, including several that appear to have been spaced out by approximately an hour. **Subject Account 1** is a Binance account, and Binance records indicate the account currently contains the equivalent of approximately $93,000 in bitcoin.

40. **Subject Account 2** is a Paxful account that controls bitcoin address 3QGWYbm8qpLpqSCMZp3RWipqa8Rwymc2ni. According to the Paxful records, **Subject Account 2** received funds from wallet bc1qlt50xpslnxwaztz7cmsp6ga5g30cs94ceyrlxr in March 2024. In March and April 2024, this bc1qlt5 wallet also sent funds to three other addresses associated with the South Korean Manufacturing Company ransom: the bc1qzcw address, discussed in paragraphs 34 and 35; the

bc1qnhs address, discussed in paragraphs 37 and 38; and the 32D4pk4 address, which previously received funds from the bc1qzcw address, discussed in paragraph 35. Paxful records indicate the account currently contains the equivalent of approximately $50,000 in bitcoin.

41. The graph in Attachment B depicts the general movement of cryptocurrency from April 2023 to April 2024. The 4.29 BTC ransom payment from South Korean Manufacturing Company to the first Andariel-controlled wallet appears in the top left. The December 2023 activity, which I have probable cause to believe was intended to conceal the nature, source, location, ownership, or control of the ransom proceeds, is displayed in the upper part of the graph. The April 2024 activity, which I also have probable cause to believe was designed to conceal the nature, source, location, ownership, or control of the ransom proceeds, makes up the majority of the graph, including the center and bottom-right parts.

42. According to Binance, **Subject Account 1** was created on June 2, 2020. According to Paxful, **Subject Account 2** was created on July 16, 2020.

43. Based on the information obtained from ransomware victims, FBI personnel, the public blockchain, and cryptocurrency exchanges, I have probable cause to believe the Andariel co-conspirators have engaged in money laundering transactions with the proceeds of the South Korean Manufacturing Company ransom that are derived from violations of 18 U.S.C. § 1030, by utilizing various cryptocurrency addresses and exchanges, as set out herein, which includes **Subject Account 1** and **Subject Account 2**.

VI. CONCLUSION

44. Based upon the foregoing, probable cause exists to believe that the contents of the Subject Accounts listed in Attachments A-1 and A-2 to this Affidavit constitute property involved in or traceable to property involved in transactions or attempted transactions in violation of 18 U.S.C. §

1956(a)(1)(B)(i) (concealment money laundering) and 18 U.S.C. § 1956(h) (conspiracy to commit money laundering). Therefore, the entire contents of **Subject Account 1** (approximately 1.3833 BTC) and the entire contents of **Subject Account 2** (approximately 0.739 BTC) are subject to seizure and forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A). Accordingly, the application for seizure warrants requests seizure of the entire contents of both accounts.

45. The FBI has confirmed that Binance and Paxful accept service of process by email. Because the U.S. Government will serve the requested warrants on Binance and Paxful by email, there exists reasonable cause to permit the execution of the requested warrants at any time in the day or night.

[redacted]
Special Agent
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this day 11th of June 2024.

Angel Mitchell
HONORABLE ANGEL D. MITCHELL
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-1: PROPERTY TO BE SEIZED

1. Binance User ID 581919046 (**Subject Account 1**), located at Binance Holdings Limited.

ATTACHMENT A-2: PROPERTY TO BE SEIZED

1. Paxful User ID 4690943 (**Subject Account 2**), located at Paxful, Inc.

ATTACHMENT B: GRAPH OF CRYPTOCURRENCY TRANSACTIONS