Exhibit A

AFFIDAVIT IN SUPPORT OF COMPLAINT FOR FORFEITURE

I, Rodrigo Fuzon, being duly sworn, depose and state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and am currently assigned to the FBI's St. Louis Field Office. Prior to my employment with the FBI, I spent 14 years as a computer systems engineer. I have been employed by the FBI since 2022 and am currently assigned to an FBI cybercrime squad in the St. Louis Field Office where I investigate national security and criminal matters. During my tenure as a Special Agent with the FBI, I have conducted numerous criminal investigations, including, but not limited to, investigations involving violations of 18 U.S.C. §§ 1030 (computer fraud and abuse), 1349 (conspiracy to commit wire fraud), 1343 (wire fraud), 1956 (money laundering and money laundering conspiracy), and 1957 (monetary transactions in criminally derived property). I have also received training and gained experience regarding the use of cellular telephones during and in furtherance of criminal activity, and searching email and other electronic accounts, including Google accounts, to ascertain evidence of criminal conduct that may be present on such accounts.

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

a. 17 electronic accounts stored at premises owned, maintained, controlled or operated by Google LLC, an internet service provider headquartered in Mountain View, California;

b. 18 electronic accounts stored at premises owned, maintained, controlled or operated by Yahoo Inc., an internet service provider headquartered in New York, New York; and

c. 2 electronic accounts stored at premises owned, maintained, controlled or operated by IONOS Inc., an internet service provider headquartered in Philadelphia, Pennsylvania.

A list detailing all 37 accounts is included in Attachment A (collectively, the "Email Accounts").

3. As set forth below, I respectfully submit that there is probable cause to believe that the Email Accounts were property used, or intended to be used, by state-sponsored malicious cyber actors to commit or facilitate violations of 18 U.S.C. § 1030 (Computer Fraud), 18 U.S.C. § 1956(h) (Conspiracy to Commit Money Laundering) and 18 U.S.C. § 2332b(g)(5) (Acts of Terrorism), and that such property is subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and (a)(1)(G).

4. The facts set forth in this affidavit are based on my personal knowledge, the knowledge obtained during my participation in this investigation, the knowledge obtained from other individuals, including other law enforcement personnel, review of documents and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. This affidavit does not contain all of the information known to me or others in regard to the investigation; however, it contains information establishing probable cause to forfeit the Email Accounts.

OVERVIEW OF THE COMPUTER INTRUSION CONSPIRACY

A. Ransomware Attack on Kansas Medical Provider

5. This investigation commenced when officials working on behalf of a healthcare provider located in Chanute, Kansas, within the District of Kansas, advised the FBI that on or around May 4, 2021, the medical provider became the victim of a ransomware attack. On or around that day, the Kansas medical provider's employees discovered they could not access computer files. Attempts to open files resulted in receipt of an error message stating that the file format had changed.

6. The Kansas healthcare provider's employees were unable to access the computer server used for x-rays and diagnostic imaging; the server used for scanning data; the internal intranet server; and the sleep lab server.

7. The Kansas healthcare 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 healthcare provider and the FBI determined that the malware was named "maui.exe" (also referred to as "the Maui ransomware").

8. The Kansas healthcare provider's information technology 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 bitcoin (also referred to as "BTC") be sent to an address supplied by the attackers. If payment was not made within 48 hours, the note stated that the price would double. Additionally, the ransom note stated, "Our email address: ReneeAFletcher@protonmail.com."

9. The FBI confirmed that on May 11, 2021, a payment for 1.66 BTC was made on the Kansas healthcare provider's behalf to the bitcoin address supplied by the attackers. The remainder of the ransom was paid on the Kansas healthcare provider's behalf to the same bitcoin address on May 17, 2021. The malicious cyber actors subsequently provided the Kansas healthcare provider the decryption keys to decrypt and access their systems and files, but only after the four servers used to provide healthcare services had all been inaccessible for over a week.

10. As part of its investigation, the FBI determined that the Maui ransomware was a type of malware that had not been reviewed by the FBI prior to the attack on the Kansas medical center. Between the initial May 2021 attack and July 2022, the FBI responded to multiple Maui ransomware incidents at other U.S. organizations in the healthcare sector. The victims of these attacks were also told to pay ransoms in bitcoin.

11. On July 6, 2022, the FBI, the Cybersecurity and Infrastructure Security Agency, and the Department of Treasury announced that the Maui ransomware was being used by North Korean ("DPRK") 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. The state-sponsored actors encrypted electronic medical records, diagnostic services, imaging services, and intranet services in these attacks, which often lasted for prolonged periods of time, according to the announcement.

B. The FBI Investigation and Identification of DPRK Malicious Cyber Actors' Tactics, Techniques, and Procedures (TTPs)

12. Following the initial report of the ransomware attack on the healthcare provider located in the District of Kansas in May 2021, the FBI analyzed the malicious cyber actors' tactics, techniques, and procedures ("TTPs"). The FBI also reviewed ransom notes, the

blockchain, and other information from victims and victim computer networks as part of its investigation. Additionally, the FBI obtained legal process on numerous email and other online accounts that have been linked to the Maui ransomware campaign.

13. The following terminology is necessary to understand how the FBI has investigated these actors, attributed computer intrusions and money laundering activity to the co-conspirators, and linked the specific accounts to be seized to the illegal activity:

a. *Cookies*. Based on my training and experience, I know that providers such as Google and Yahoo use cookies and similar technologies to track users visiting their webpages and using their products and services. Basically, a "cookie" is a small file containing a string of characters that a website places 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 and Yahoo. More sophisticated cookie technology can be used to identify users across devices and web browsers. From my training and experience, I know that cookies and similar technology used by providers such as Google and Yahoo 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 or Yahoo account and determine the scope of the criminal activity.

b. *IP addresses*. Every device that connects to the Internet must use an Internet Protocol (IP) address. Because of this, IP address information can help to

identify which computers or other devices were used to access a particular account. Providers, including Google and Yahoo, log the IP addresses used to register accounts and the IP addresses users use to login to their accounts.

c. *Recovery email addresses*. Based on my training and experience, I know that a recovery email address is used to regain control of an email address if the user forgets the password. When a user registers an account with Google, Yahoo, or Proton Mail (an email product provided by the Swiss company Proton Technologies AG), they generally provide such a recovery email address. These providers will often verify recovery email addresses by sending a code to the recovery email and having the user enter that code to complete the registration of the recovery email. Therefore, I know that the user of an account generally has access to and control of the recovery email address.

d. *Secondary and alternate email addresses*. Based on my training and experience, I know that email services often allow users to be logged into more than one account at the same time or use other methods to associate multiple accounts. These accounts are often referred to as secondary or alternate email addresses.

e. *Recovery phone numbers*. Based on my training and experience, I know that providers including Google and Yahoo collect phone numbers for multiple purposes, including to be used for SMS two-factor authentication. These providers will often verify phone numbers by sending a code and having the user enter it on their browser. I know from my training and experience that, when multiple accounts share the same recovery phone number, they are generally controlled by the same person.

14. I know from my training and experience that malicious cyber actors often create large numbers of accounts at email and communications providers, web hosting providers, and cryptocurrency providers, in an attempt to compartmentalize their operations and make it more difficult to trace different intrusions to the same threat actor. Even so, multiple accounts can often be traced to the same threat actor when, for example, they (1) have been accessed from the same Internet Protocol (IP) address, (2) are used as recovery, secondary, or alternate email addresses, (3) are linked by cookies, (4) use the same phone number, or (5) use the same moniker or username. In this investigation, the FBI has identified a large number of email addresses associated with the same group of malicious cyber actors.

15. I know from my training and experience that providers of email services, web hosting services, cryptocurrency exchanges and payment services, and file storage services collect information about their users, such as IP addresses and cookie information, and often require their users to affirmatively provide and verify contact information, such as recovery email addresses and phone numbers.

16. Some TTPs of these DPRK malicious cyber actors are distinct. I have learned from the investigation that these actors create large numbers of online accounts, including accounts that provide encrypted services. These online accounts are often linked by cookie, IP address, recovery, secondary, or alternate email address, or phone number; it is generally much easier to create a new email address than to obtain a new valid phone number or a new device. Throughout the investigation, the FBI identified accounts accessed by IP addresses located in the DPRK.

17. According to information from victims and exfiltrated data, including data hosted in cloud storage accounts controlled by the malicious cyber actors, these actors have specifically

targeted United States and South Korean entities with Maui ransomware. This is consistent with industry reporting. The FBI has concluded that the malicious cyber actors responsible for the Maui ransomware campaign are part of a group known to private sector security researchers as Andariel, Onyx Sleet, Stonefly, and Silent Chollima. Private sector researchers consider Andariel to be a subgroup of Lazarus Group, which is closely tied to the DPRK regime.

18. The FBI has determined that the use of the Maui ransomware and the laundering of the ransoms is one part of Andariel's operations. According to open-source reporting, ransom payments obtained by Andariel are transferred among various cryptocurrency accounts and ultimately used as a source of income for the DPRK government. Based on the FBI investigation, these malicious cyber actors are working on behalf of the DPRK government's Reconnaissance General Bureau ("RGB").

19. In addition to this type of ransomware and money laundering activity, private sector security researchers and the FBI have observed this group of malicious cyber actors and the RGB engaging in espionage against key government entities and defense contractors in the United States, South Korea, and other Western countries. Information obtained during this investigation indicates that Andariel has committed ransomware attacks against at least five U.S.-based healthcare entities and then used the proceeds to finance its espionage operations. RGB actors have succeeded in these operations, exfiltrating terabytes of data such as research, plans, intellectual property, and other confidential business and government information from victims across the world in the pharmaceutical, defense, and technology sectors. The government previously served legal process on U.S. providers for DPRK-controlled accounts that contained exfiltrated victim data.

PROBABLE CAUSE

Google Accounts

20. On May 4, 2021, the FBI responded to the healthcare provider in the District of Kansas that was hit by a ransomware attack—an attack later determined to be the first known Maui attack. In coordination with the healthcare provider's information technology team, the FBI learned that the malicious cyber actors provided an email address to negotiate the ransom with the victim: ReneeAFletcher@protonmail.com.

21. The United States made a Mutual Legal Assistance Treaty ("MLAT") request to Switzerland for Proton Technologies AG records related to the email address ReneeAFletcher@protonmail.com. Records received from Proton Technologies AG showed that the account ReneeAFletcher@protonmail.com was created on June 29, 2019, with the recovery email address whas1985@yahoo.com.

22. In December 2021, January 2022, and April 2022, search warrants were executed on the account whas1985@yahoo.com. Through these warrants, the FBI was able to determine that the whas1985@yahoo.com account was primarily being used by a DPRK-sponsored malicious cyber actor to communicate with co-conspirators conducting malicious cyber activity, including to (1) plan ransomware attacks, and (2) send bitcoin transaction information in order to launder the extorted funds.

23. For example, the email account raajivkum26@gmail.com sent an email to whas1985@yahoo.com. The government served legal process on Google to identify subscriber records for the account raajivkum26@gmail.com. This account was identified as being created on May 9, 2019, under the name Rajiv Kumar. This account also used a recovery email account

of tomson.wedner@mail.com (discussed below). The FBI obtained a search warrant for Google account raajivkum26@gmail.com.

24. The government identified one email in the search warrant return, sent from raajivkum26@gmail.com to whas1985@yahoo.com on July 4, 2022. This email had a subject of "Hi" and contained an encoded string of characters. The FBI decoded this string and identified it as a bitcoin address. The FBI analyzed the bitcoin address and learned that it received a payment on July 5, 2022 (the day after the message was sent).

25. The government linked this transaction to proceeds from a ransomware payment made by a healthcare company victim located in the District of Connecticut. The ransomware attack on this victim used malware that functioned similarly to Maui ransomware and was called m.exe.

26. The government previously obtained a search warrant for Google accounts songvedembmt1@gmail.com, daviddpedroo999@gmail.com, david.0000.paul@gmail.com, kopasrsele@gmail.com, coinhakohuobi@gmail.com, and kasurkurma20feb@gmail.com. These accounts were linked by cookies to raajivkum26@gmail.com, indicating that the same device was used to access these different Google accounts. The Google search warrant return showed that Google account busisyhasi@gmail.com was linked by cookie and recovery email to daviddpedroo999@gmail.com. Additionally, the search warrant returns showed that Google accounts jamie.dornan05@gmail.com was linked by cookies to david.0000.paul@gmail.com.

27. The government previously obtained a search warrant for Google account asitdolui6666@gmail.com. This account was also linked by secondary email to raajivkum26@gmail.com and by recovery email to kopasrsele@gmail.com. Additionally, both

raajivkum26@gmail.com and asitdolui6666@gmail.com have the same recovery email: tomson.wedner@mail.com (discussed below).

28. The government previously obtained a search warrant for the account tayronqxhardy07@gmail.com. In addition to being linked to other Andariel-controlled Google accounts by cookie and to the same IP address as other accounts, tayronqxhardy07@gmail.com was also the email address provided by DPRK co-conspirators to a South Korean victim company in March 2023 for ransomware negotiations. tayronqxhardy07@gmail.com used the same recovery account as another known Andariel Google account.

29. Lee Boreas is a known moniker of the DPRK-sponsored cyber actors. The FBI obtained a pen register/trap-and-trace order and search warrant for the account leeboreas@gmail.com. The account has been linked to other DPRK accounts in various ways and has communicated with other known malicious DPRK cyber actors, including whas1985@yahoo.com. The search warrant return for leeboreas@gmail.com indicated that the user of the account has searched for terms related to secure messaging applications and virtual private network (VPN) products. Additionally, an email between leeboreas@gmail.com and whas1985@yahoo.com discusses the procurement of a technology product and a "bit-c transaction." From my training and experience, including my experience on this investigation, I interpret "bit-c transaction" as a reference to a bitcoin transaction, which likely relates to these malicious actors' laundering of ransom payments.

30. The government previously obtained search warrants for Google accounts vkr5731@gmail.com and duttapritom78@gmail.com. A review of the search warrant returns indicates that these accounts both use the same recovery phone number as whas1985@yahoo.com. Additionally, vkr5731@gmail.com and duttapritom78@gmail.com,

respectively, use the same phone numbers as letitiajpoland@yahoo.com and jainathmanoj@yahoo.com. Both letitiajpoland@yahoo.com and jainathmanoj@yahoo.com are linked by cookies to whas1985@yahoo.com. These Yahoo accounts are discussed next.

31. The government previously obtained a pen register/trap-and-trace order for Google account nirmhanpandiri@gmail.com. The nirmhanpandiri@gmail.com account has been associated with Andariel activity related to the Tdrop malware, which is a Microsoft Windows malware family widely attributed by the private sector to North Korea. According to records previously obtained from hosting providers and Yahoo, nirmhanpandiri@gmail.com was the recovery email address for a Yahoo email address used to register command-and-control servers used in Andariel's Tdrop attacks. The Andariel actors created a large number of Yahoo accounts, possibly as an obfuscation tactic. This Google account, nirmhanpandiri@gmail.com, is also linked by cookie to another known Andariel account, indicating that it is likely controlled by the same Andariel actor.

32. An Andariel victim company received a ransom note from email address sanjgold847@protonmail.com. The government requested and received records from Proton Technologies AG, which showed that the account sanjgold847@protonmail.com has a recovery email of nicolas6999999@gmail.com.

33. The government previously obtained a search warrant for Google account reneefletcher1988@gmail.com. This account uses a similar moniker to the email provided to the victim in the first Maui ransomware attack, ReneeAFletcher@protonmail.com. Furthermore, the search warrant return indicated that whas1985@yahoo.com was the recovery email for reneefletcher1988@gmail.com. It also showed that a similarly named account, reneeafletcher@mail.com (discussed below), was in the contact list of

reneefletcher1988@gmail.com. Additionally, the search warrant return also contained emails received from blockchain.com and Shodan, a type of search engine that can scan the internet for vulnerable internet-connected devices.

Yahoo Accounts

34. As set forth above, whas1985@yahoo.com is directly tied to the first Maui ransomware attack on the Kansas healthcare provider. (See, ¶ 21). The malicious cyber actors provided email address ReneeAFletcher@protonmail.com to the victim. As part of the investigation, the United States requested records related to ReneeAFletcher@protonmail.com. Records from Proton Technologies AG showed that the account was created on June 29, 2019, with the recovery email address whas1985@yahoo.com. The government previously obtained multiple search warrants for whas1985@yahoo.com and determined it is one of the primary accounts used by the malicious cyber actors to conduct ransomware and espionage operations.

35. As a result of those warrants, the government learned that the malicious cyber actor who controlled whas1985@yahoo.com received multiple emails from wj0705@yahoo.com. The government obtained multiple search warrants on wj0705@yahoo.com, which is believed to be used by a co-conspirator. The FBI reviewed emails, including emails between both of these accounts, and determined the co-conspirators in many cases used coded messages. The government also obtained a pen register/trap-and-trace order on wj0705@yahoo.com in 2022.

36. As a result of legal process, the FBI learned that rajusandhipeta@yahoo.com is linked by cookies to whas1985@yahoo.com.

37. The government previously sought and received a search warrant for Yahoo account rajeshchatarghi@yahoo.com. This was the recovery account for

gregorykcortes@protonmail.com, which was used to send a ransom note to a foreign Maui ransomware victim. Additionally, rajeshchatarghi@yahoo.com used a recovery phone number known by the FBI to be controlled by DPRK malicious cyber actors.

38. That same DPRK-controlled phone number was also used as a recovery phone number for the accounts murthyvenu@yahoo.com and rudhraduppatla@yahoo.com, which are both believed to be controlled by the same DPRK malicious cyber actor.

39. The government previously obtained a search warrant for Yahoo account jeevanmannepu@yahoo.com. This email address was linked to the Maui ransomware actors and an attack on a Colorado medical provider through cryptocurrency tracing, Binance records, and records from Proton Technologies AG. The malicious file in that attack was named "aui.exe."

40. The FBI previously sought and received search warrants for the contents of the Yahoo accounts kiranvanasathi@yahoo.com, letitiajpoland@yahoo.com, jainathmanoj@yahoo.com, and ramsethul@yahoo.com. All four of these accounts were linked by cookies to whas1985@yahoo.com.

41. The government previously obtained search warrants for the contents of the Yahoo accounts vardhan_girish@yahoo.com, kiranvaghi@yahoo.com, nandhankorada@yahoo.com, karthivalasa@yahoo.com, raginishraina@yahoo.com, pranithkanakala@yahoo.com, and shivanghjain@yahoo.com. All of these accounts use the same recovery phone number as kiranvanasathi@yahoo.com, which is linked by cookie to whas1985@yahoo.com.

IONOS (mail.com) Accounts

42. Upon reviewing search warrant results for whas1985@yahoo.com, the FBI discovered that email address reneeafletcher@mail.com was in the contact list. This account

uses the same moniker, "Renee A. Fletcher," that was used in the protonmail.com email address left in the May 2021 ransom note to the Kansas victim.

43. The government previously sought and obtained a warrant for IONOS account tomson.wedner@mail.com. As previously discussed, both raajivkum26@gmail.com and asitdolui6666@gmail.com use the recovery account tomson.wedner@mail.com.

44. On July 24, 2024, seizure warrants were obtained and served on all three providers directing them to suspend user access to the Email Accounts, thereby "locking" the accounts and preventing user access to and manipulation of the contents of the account.

45. On July 25, 2024, Google LLC confirmed the suspension of the 17 electronic Google accounts identified in the investigation.

46. On July 25, 2024, Yahoo Inc. confirmed the suspension of the 18 electronic Yahoo accounts identified in the investigation.

47. On July 25, 2024, IONOS, Inc. confirmed the suspension of the two electronic IONOS account identified in the investigation.

CONCLUSION

48. Based upon the foregoing information, there is probable cause to believe that the Email Accounts are subject to civil forfeiture because they were used or intended to be used to commit or to facilitate the commission of 18 U.S.C. § 1030 (Computer Fraud), 18 U.S.C. § 1956(h) (Conspiracy to Commit Money Laundering) and 18 U.S.C. § 2332b(g)(5) (Acts of Terrorism). Specifically, the Email Accounts were involved in and enabled the North Korean state-sponsored malicious cyber activity, including ransomware attacks on and extortion of U.S. healthcare providers and subsequent money laundering of the ransoms.

49. Accordingly, I have probable cause to believe that the Email Accounts constitute "property, real or personal, involved in a transaction or attempted transaction in violation of section 1956 . . . or any property traceable to such property" and are, therefore, subject to forfeiture under 18 U.S.C. § 981(a)(1)(A).

50. Additionally, I have probable cause to believe that the Email Accounts were involved in, used, or intended to be used to commit ransomware attacks on healthcare providers by the North Korean Reconnaissance General Bureau, in violation of 18 U.S.C. §§ 2332b(g)(5) and 1030(a)(5)(A) and (c)(4)(A)(i)(II). The attacks were "calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct," (18 U.S.C. § 2332b(g)(5)(A)), and they caused "the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals," (18 U.S.C. § 1030(c)(4)(A)(i)(II)), when they encrypted computers belonging the healthcare facilities within the United States. Because the Email Accounts are assets "derived from, involved in, or used or intended to be used to commit any Federal crime of terrorism (as defined in section 2332b(g)(5)) against the United States, citizens or residents of the United States, or their property," they are subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(G)(iii).

51. Because all assets of any individual, entity, or organization engaged in planning or perpetrating any Federal crime of terrorism (as defined in 18 U.S.C. § 2332b(g)(5)), which includes violations of 18 U.S.C. § 1030), against the United States, citizens or residents of the United States, or their property are subject to forfeiture,, I have probable case to believe that the Emails Accounts are also forfeitable pursuant to 18 U.S.C. § 981(a)(1)(G)(i).

Rodrigo Fuzon
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me this 27TH day of February, 2026.

MEGAN ANN MAIER
Notary Public - Notary Seal
STATE OF MISSOURI
St. Louis City
My Commission Expires Dec. 20, 2029
Commission #21029814

2/27/2026
Notary Public