

UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Seizure of
All money, funds, and financial instruments
deposited or credited to certain [REDACTED]
accounts, further described in Attachment A

)
)
)
)
)

Case No. 4:24 MJ 1240 JMB

APPLICATION AND AFFIDAVIT FOR SEIZURE WARRANT

I, [REDACTED], being duly sworn depose and say:

I am a Special Agent with the Federal Bureau of Investigation, and have reason to believe that there is now certain property namely

All money, funds, and financial instruments deposited or credited to certain [REDACTED] accounts, further described in Attachment A

which is

subject to forfeiture under Title 18, United States Code, Sections 981(a) and 982(a) and Title 28, United States Code, Section 2461, and therefore, is subject to seizure under Title 18, United States Code, Sections 981(b)& 982(b) and Title 21, United States Code, Sections 853(e)&(f) concerning a violation of Title 18, United States Code, Section 1956 and Title 50, United States Code, Section 1705.

Because the violation giving rise to this forfeiture occurred within the Eastern District of Missouri, this Court is empowered by 18 U.S.C. § 981(b)(3) and 28 USC § 1355(d) to issue a seizure warrant which may be executed in any district in which the property is found. The seized property is to be returned to this district pursuant to 28 U.S.C. § 1355(d).

The funds identified herein are subject to civil forfeiture without regard to their traceability to criminal activity because they are contained in an account into which identical traceable property has been deposited and therefore may be forfeited as fungible property under Title 18, United States Code, Section 984.

The facts to support a finding of Probable Cause for issuance of a Seizure Warrant are as follows:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

Continued on the attached sheet and made a part hereof.

X Yes ____ No

[REDACTED]
Signature of Affiant, Special Agent [REDACTED]

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41

July 18, 2024 10:00 a.m.
Date and Time Issued

at St. Louis, Missouri
City and State

Honorable John M. Bodenhause, U.S. Magistrate Judge
Name and Title of Judicial Officer

[REDACTED]

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEIZURE WARRANT

I, [REDACTED], a Special Agent with the Federal Bureau of Investigation (“FBI”), being duly sworn, depose and state as follows:

1. I am a Special Agent at the Federal Bureau of Investigation (“FBI”). I have been a Special Agent with the FBI since [REDACTED] 2007. Since April 5, 2010, I have been assigned to a cyber squad in the FBI’s St. Louis Field Office. I have received training regarding computer fraud and computer hacking. I have conducted investigations into various forms of online criminal activity and am familiar with the ways in which such crimes are commonly conducted. In addition, I have participated in the execution of search warrants involving electronic evidence.

2. 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.

3. This affidavit does not contain all of the information known to me in regard to the investigation; however, it contains information establishing probable cause to seize approximately \$444,828.01 held in the nine specific [REDACTED] (“Payment Service Provider 1”) accounts listed in Attachment A (the “**Target Accounts**”). Payment Service Provider 1 is a U.S. based financial services company that provides online money transfer and digital payment services to its customers, who can use their Payment Service Provider 1 account to receive, store, and send money, including to counterparties from outside of the Payment Service Provider 1 network.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that unknown foreign persons have committed violations of 50 U.S.C. § 1705(a) (International Emergency Economic Powers Act, or “IEEPA”), 18 U.S.C. § 1349 (Conspiracy to Commit Wire Fraud), 18 U.S.C. § 1028A (Aggravated Identity Theft) and 18 U.S.C. § 1956 (Money Laundering) (the “Subject Offenses”). This includes performing online freelance information technology work for North Korea in violation of IEEPA.

5. I submit that there is probable cause to seize the funds in the **Target Accounts** because they were used to conceal or disguise the nature, location, source, ownership, or control of the proceeds of IEEPA violations and wire fraud. *See* 18 U.S.C. §§ 1956(a)(3)(B) (Money Laundering) and 981(a)(1)(C) (Civil Forfeiture). Because the **Target Accounts** are subject to civil and criminal forfeiture, they may be seized pursuant to 18 U.S.C. § 981(b) and 21 U.S.C. § 853(f). The procedure by which the government will seize the Subject Domain Names is described in Attachment A and below.

APPLICABLE STATUTES

I. International Emergency Economic Powers Act (IEEPA)

6. The International Emergency Economic Powers Act (IEEPA), enacted in 1977 and codified at 50 U.S.C § 1701 et seq., authorizes the President of the United States (the “President”), among other things, to impose economic sanctions in response to an unusual or extraordinary threat to the national security, foreign policy, or economy of the United States. Pursuant to that authority, the President may declare a national emergency through Executive Orders with respect to that threat; those Executive Orders have the full force and effect of law. It is a crime to willfully violate, attempt to violate, conspire to violate, or cause the violation of any license, order, regulation, or prohibition issued pursuant to IEEPA. 50 U.S.C. § 1705(a).

7. Beginning with Executive Order 13466, issued on June 26, 2008, the President found the situation “on the Korean Peninsula constitute[s] an unusual and extraordinary threat to the national security and foreign policy of the United States and . . . declare[d] a national emergency to deal with that threat.”

8. On March 15, 2016, the President, in order to take additional steps with respect to the previously described national emergency, issued Executive Order 13722 addressing the Government of North Korea’s continuing pursuit of its nuclear and missile programs. Executive Order 13722 imposed a comprehensive blocking of the Government of North Korea and the Workers’ Party of Korea. Pursuant to that authority, on March 5, 2018, the Secretary of the Treasury amended the “North Korea Sanctions Regulations.” [83 Fed. Reg. 9182 \(Mar. 5, 2018\)](#); see [31 C.F.R. § 510.101](#) et seq. Executive Order 13722 and the North Korea Sanctions Regulations prohibit the export of financial services from the United States or by any U.S. person to North Korea, unless exempt or authorized by the U.S. Department of Treasury’s Office of Foreign Assets Control (“OFAC”). Under these orders, U.S. financial institutions were barred from providing correspondent banking services to North Korea entities.

9. OFAC administers and enforces economic sanctions programs established by executive orders issued by the President pursuant to IEEPA. Pursuant to Executive Order 13722, OFAC has the authority to block all property and interests in property that are in the United States, that hereafter come within the United States, or that are or hereafter come within the possession or control of any United States person or persons who meet specific criteria.

10. On September 13, 2018, OFAC designated a North Korean information technology firm based in China named Yanbian Silverstar Network Technology Co., Ltd (“Yanbian Silverstar”), as well as its Russia-based front company, Volasys Silver Star, for

having engaged in, facilitated, or been responsible for the exportation of workers from North Korea, including exportation to generate revenue for the Government of North Korea or the Workers' Party of Korea, pursuant to Executive Order 13722, and for operating in the IT industry in North Korea, pursuant to Executive Order 13810. OFAC further designated a North Korean national, Jong Song Hwa, identified by OFAC as the CEO of Yanbian Silverstar and Volasys Silver Star.

11. According to the OFAC designation press release, the sanctioned parties channeled "illicit revenue to North Korea from overseas information technology workers disguising their true identities and hiding behind front companies, aliases, and third-party nationals." In other words, the sanctioned parties were conspiring to create and use pseudonymous email accounts, social media accounts, payment platform accounts, websites, and online job site accounts to obfuscate their true identities as North Koreans, and to solicit and perform information technology freelance jobs to earn money for the North Korean government in violation of U.S. sanctions.

II. Civil and Criminal Forfeiture

12. Pursuant to 18 U.S.C. § 981(a)(1)(C) & (D)(vi) and 28 U.S.C. § 2461(c), any property, real or personal, which "constitutes or is derived from proceeds traceable" to (i) a "specified unlawful activity" within the meaning of the money laundering statute (18 U.S.C. § 1956(c)(7)) to include violations of 50 U.S.C. § 1705, is subject to forfeiture.

13. 18 U.S.C. § 981(a)(1)(C) & (D)(vi) (civil forfeiture) provides for the forfeiture of any property, real or personal, involved in a transaction or attempted transaction in violation of, inter alia, 18 U.S.C. § 1956, as well as any property traceable to such property.

14. 18 U.S.C. § 982(a)(1) (criminal forfeiture) provides that, as part of the sentence

for a violation of, inter alia, 18 U.S.C. § 1956, the Court shall order the forfeiture of any property, real or personal, involved in the offense or any property traceable to that property.

15. Pursuant to 18 U.S.C. § 981(b) (civil seizure), property subject to civil forfeiture may be seized by a 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. A civil forfeiture action may be brought in any district where “acts or omissions giving rise to the forfeiture occurred.” 28 U.S.C. § 1355(b)(1)(A).

16. 21 U.S.C. § 853(f) (criminal seizures) authorizes the seizure of property subject to criminal forfeiture based upon a warrant supported by probable cause where the property to be seized would, in the event of conviction, be subject to forfeiture.

17. Seeking a restraining order under 21 U.S.C. § 853(e) may not be sufficient to assure the availability of the property for forfeiture because there is reason to believe that the property is under the control of the targets of this investigation, who cannot reasonably be relied upon to abide by an order to maintain the property in substantially the same condition as it is at the present time, in order to ensure that it will be available for forfeiture. More particularly, providing notice may allow the targets to frustrate further efforts of law enforcement by transitioning their enterprise and infrastructure to jurisdictions beyond the reach of United States law enforcement.

BACKGROUND REGARDING NORTH KOREAN INFORMATION TECHNOLOGY WORKERS

18. According to a May 16, 2022, report jointly issued by the U.S. Department of State, U.S. Department of the Treasury, and the FBI, North Korea uses freelance information technology workers to generate a revenue and foreign currency stream for its weapons of mass

destruction and ballistic missile programs.

19. The freelance North Korean IT workers deceive their employers by buying, stealing, or counterfeiting the identities and mailing addresses of non-North Koreans when bidding on and completing freelance projects, in order to conceal their identities as North Koreans.

20. North Korean IT workers also either pay or deceive non-North Koreans to interview for jobs for them, accept payment for freelance projects, and videoconference with their employers when necessary. These non-North Koreans may not be aware that the IT workers are North Korean.

21. North Korean IT workers use multiple accounts and multiple freelance contracting platforms, digital payment platforms, social media and networking applications, and email and messaging applications, in order to obtain and perform IT contracts, receive payment for their work, and launder those funds. North Korean IT workers also create software development companies to hire other developers and provide a presence on the internet to bolster their legitimacy and mask their true identities. These “portfolio websites” allow North Korean IT workers to showcase previous development activity and generate freelancer jobs.

22. The North Korean IT workers are often located in China and Russia. In order to avoid suspicion that they are North Korean and be able to use U.S.-based online services, North Korean IT workers use virtual private networks, virtual private servers, and proxy IP addresses to make it appear that they are connecting to the internet from false locations. North Korean IT workers also use remote desktop software to access U.S.-based computers to make it appear as though they are connecting to online services from different locations.

**FACTS ESTABLISHING PROBABLE CAUSE TO BELIEVE
CRIMES HAVE BEEN COMMITTED**

23. In August 2019, the FBI interviewed an individual (“Individual 1”) who had allowed another person, subsequently identified as a North Korean IT worker working for Yanbian Silverstar, to use Individual 1’s online account at a U.S. based freelancer platform. Additionally, Individual 1 allowed the North Korean IT worker to remotely access laptops at Individual 1’s residence in the United States for freelance work, and the North Korean IT worker paid Individual 1 \$100 per month per hosted laptop.

24. The investigation subsequently identified hundreds of financial and communication accounts associated to Yanbian Silverstar and other North Korean IT worker groups. In February 2022 and July 2022, United States Magistrate Judges Shirley P. Mensah and John M. Bodenhausen in the Eastern District of Missouri signed search warrants for numerous Google and Microsoft accounts associated with Yanbian Silverstar actors. The communications from these Google and Microsoft accounts discussed using identities of U.S. citizens and individuals based around the world to open accounts at payment and freelancer platforms. They also used Korean language and North Korean honorifics to communicate with each other. Those communications clearly identified them as North Koreans doing IT work on behalf of North Korea.

25. On October 25, 2022, January 19, 2023, and January 11, 2024, seizure warrants were issued by the Eastern District of Missouri for funds held in accounts controlled by North Korean IT workers at Payment Service Provider 1.

26. In December 2023, the FBI reviewed reports provided by Payment Service Provider 1 which identified suspected accounts associated with North Korean IT worker activity. The FBI concluded that 387 of these accounts were likely used to facilitate North Korean IT

worker financial transactions. The **Target Accounts** that are the subject of this affidavit were among these accounts. The FBI concluded that all 387 accounts were likely controlled by North Korean IT workers because they engaged in some or all the following suspicious activities:

- i. New bank accounts were created using names that were different from the original account holder;
- ii. The identity documents and/or verification documents used to create new accounts were likely fake or stolen;
- iii. Multiple email addresses were used and the names in those emails were not the account holder's name;
- iv. Chinese bank accounts were used to register accounts with Payment Service Provider 1 from countries other than China;
- v. Logins from IP addresses occurred from locations where North Korean IT workers operate;
- vi. Logins occurred from IP addresses affiliated with Virtual Private Network ("VPN") services or proxy IP addresses that North Korean IT workers regularly use;
- vii. Payments occurred from freelance companies and staffing firms to individuals with different names, all of whom were using the same Payment Service Provider 1 account; and
- viii. There were recurring withdrawals from the Payment Service Provider 1 account to Chinese bank accounts in \$10,000 or \$20,000 increments.

27. The nine **Target Accounts**, all provided by Payment Service Provider 1, contain \$444,828.01 in proceeds from the IT workers' criminal scheme, and they are further described

below.

I. Account Holder ID: 39566449 (Target Account 1)

28. Payment Service Provider 1 Account Holder ID: 39566449 (**Target Account 1**) has an outstanding balance of \$239,927.62. It has the following account information:

Name: [REDACTED]
Address: [REDACTED]
Email: [REDACTED]@163.com
Registration Date: 08/22/2020

29. From November 2021 to June 2023, **Target Account 1** received \$1,016,084.43 from various companies known to the FBI. The funds appear to be payments for freelance work completed by 13 different identities. At least four of these identities had the same last name, [REDACTED] but had different first names – Jake, Jason, Mark, and Thomas. Based on my training and experience, the use of the same last name with different generic first names indicates that all the identities associated with an account are fake. Based on my training and experience, the fake identities used to set up these accounts are often different than the ones that applied for work. As a result, the FBI does not know what information was used to obtain work at the victim companies.

30. **Target Account 1** withdrew a total of \$810,000.00 to a bank account at the [REDACTED] [REDACTED] – a Hong Kong based bank – in \$10,000 increments. The money movement and withdrawals are consistent with an account used by North Korean IT workers to launder the proceeds of criminal violations. If this was normal freelance work, the data would show just one individual with one identity receiving payments from one, maybe two, jobs. Having numerous (likely fake or inaccurate) identities receiving regular payments from multiple employers to one primary bank account, indicates that the owner of that account is trying to hide the proceeds of

this activity from the United States.

31. When opening an account, Payment Service Provider 1 requires the account holders to answer questions to receive payments. The **Target Account 1** account holder stated they use the account to receive payments for web programming and stated “we provide website and application construction to service to global enterprises, which are mainly companies from USA, Canada, Australia and UK”. **Target Account 1**’s owner provided the URL for their business as [REDACTED]. A review of public records associated with the domain identified that [REDACTED] was created on or about March 24, 2020, and expired on March 24, 2023.

32. I know from my training and experience that North Korean IT workers frequently create websites to advertise their IT services and to verify accounts. Since the domain expired in March 2023 but **Target Account 1** continued to receive payments for freelance work, I believe the domain was created to verify an account with Payment Service Provider 1.

33. As part of its know your customer policies, Payment Service Provider 1 requires an account holder to provide invoices and communications associated with payments to the account. Payment Service Provider 1 does this to ensure account holders can verify the source of their income. A review of the documents provided by **Target Account 1**’s owner to Payment Service Provider 1 show that the names (totaling 13) and email addresses associated with invoices were not the account holder’s name and email address. For example, several invoices correctly listed the account holder name as [REDACTED] but stated that the individuals being paid were “[REDACTED]”, “[REDACTED]”, and “[REDACTED]”.

34. North Korean IT workers frequently tell employers they have a “financial manager” who receives their payments since they work for a team or company. The

team/company and financial manager are North Koreans utilizing the identity of an account holder. This setup allows the same North Korean IT worker to use multiple personas across the same or different employers and have payments deposited into one account. This increases their ability to generate revenue and allows the North Korean IT worker's manager to control the funds.

35. Further, in some of the documents (chats, emails, etc.) provided by the account holder to Payment Service Provider 1 to comply with Payment Service Provider 1's know your customer policies, the employers have profile pictures, but none of the IT worker personas have a picture. Based on my training and experience, I know North Korean IT workers will normally not show their faces or images in chats – unlike employers – because they do not want to be identified as Korean and associated with North Korea.

36. A review of the IP logs for **Target Account 1** identified that the user primarily logged in from VPN or proxy IP addresses which resolved to Japan and Hong Kong, and only twice from Shenyang, China, the purported location of the account holder. North Korean IT workers frequently utilize VPNs or proxy services to mask their true location. North Korean IT workers will also attempt to use IP addresses that are consistently associated with the same or similar locations when accessing an account to try to avoid getting the account flagged for suspicious or fraudulent activity. In other investigations, the FBI has observed North Korean IT workers use these same IP addresses and proxy services.

37. Based on this activity, I submit that probable cause exists to believe that **Target Account 1**, was being used by North Korean IT workers to launder the money they obtained from their criminal violations. Thus, I respectfully submit that there is probable cause to believe that the account contains property, real or personal, which “constitutes or is derived from

proceeds traceable” to a “specified unlawful activity.” See [18 U.S.C. § 981\(a\)\(1\)\(C\)](#).

II. Account Holder ID: 51679820 (Target Account 2)

38. Payment Service Provider 1 Account Holder ID: 51679820 (**Target Account 2**) has an outstanding balance of \$136,604.67 with the following account information:

Name: [REDACTED]
Address: [REDACTED]
Email: [REDACTED]
Registration Date: 04/07/2022

39. From May 2022 to June 2023, **Target Account 2** received \$1,079,692.93 from 38 companies for suspected freelance work in 38 different names, and from April 2022 to June 2023, **Target Account 2** withdrew a total of \$1,049,700.00 to a bank account at the [REDACTED] in increments of \$20,000. From April 2022 to December 2022, **Target Account 2** received \$48,850.00 from other Payment Service Provider 1 accounts located in Ukraine, China, and Vietnam – transactions I believe to be associated with other jobs held by the account owner.

40. Based on my training and experience, having 38 different names associated with one account, having that account receive payments from 38 different companies, and having that account received funds from different Payment Service 1 accounts is consistent with **Target Account 2** being used by North Korean IT workers to launder the proceeds of their criminal violations. If this was normal freelance work, the data would show just one individual with one identity receiving payments from one, maybe two, jobs. Having numerous (likely fake or inaccurate) identities receiving regular payments from multiple employers to one primary bank account, indicates that the owner of **Target Account 2** is trying to hide the proceeds of this activity from the United States.

41. Additionally, I observed that the user of **Target Account 2** made “py” the correct

answer to a security question designed to confirm his identity. These questions and answers are used by the account holder to reset or login to the account. The FBI has observed North Koreans use “py” in other contexts to refer to Pyongyang, the capital of North Korea.

42. **Target Account 2** was also linked to an [REDACTED] [REDACTED] bank account with the number [REDACTED]. Another Payment Service Provider 1 account associated with the 387 accounts identified by Payment Service Provider 1 was also identified using the same bank account. That account was in a different name and for an individual who purported to be in Sri Lanka. I know from my training and experience that the use of a Chinese bank account for payment accounts outside of China is a common tactic for North Korean IT workers. They recruit or use the identities of individuals from many different countries to open accounts at financial institutions. Once those accounts are operational, the North Korean IT worker will link those other accounts to a Chinese bank account.

43. To verify to Payment Service Provider 1 that his account was not being used to commit fraud, the owner of **Target Account 2** provided multiple invoices. All of these appeared similar but listed different developer names with the name “[REDACTED]” listed in parentheses next to each name. Based on my training and experience, I know North Korean IT workers use different identities when they work for different companies but share the same bank account for payments. This is done by the North Korean IT workers’ boss to ensure the boss controls what happens to the funds after the IT Workers are paid.

44. A review of the IP logins for **Target Account 2** identified connections to an account seized from Payment Service Provider 1 in January 2024. On June 6, 2023, the IP address [REDACTED] (South Korea) was used to log into **Target Account 2**. Approximately 5 minutes later, a login from the same IP address occurred on an account with the Account

Holder ID: 57076178 (the “57076178 Account”). This account was seized pursuant to a warrant issued on January 1, 2024, in the Eastern District of Missouri by Magistrate Judge Rodney H. Holmes. As described in the affidavit in support of the warrant to seize the 57076178 Account, the 57076178 Account received \$706,653.48 USD from various companies for suspected freelancer work in 23 different names and withdrew a total of \$422,345.00 USD to a bank account at the [REDACTED], in \$20,000 USD increments. The Court found that there was probable cause to conclude that this money movement was consistent with an account being used by North Korean IT workers to launder money.

45. In addition to the IP address logs, Payment Service Provider 1 provided the FBI with a hash or unique fingerprint of the computer used to create and access both **Target Account 2** and the 57076178 Account. For these two logins, each account shared the same fingerprint, and therefore were accessed from the same computer. The accessing of two different accounts from the same computer on the same day shows the same North Korean IT worker controlled both accounts.

46. Based on this activity, I submit that probable cause exists to believe that **Target Account 2**, was being used by North Korean IT workers to launder the money they obtained from violating IEEPA. Thus, I respectfully submit that there is probable cause to believe that **Target Account 2** contains property, real or personal, which “constitutes or is derived from proceeds traceable” to a “specified unlawful activity.” See [18 U.S.C. § 981\(a\)\(1\)\(C\)](#).

III. Account Holder ID: 54302706 (Target Account 3)

47. Payment Service Provider 1 Account Holder ID: 54302706 (**Target Account 3**) has an outstanding balance of \$16,537.21 with the following account information:

Name: [REDACTED]

Address: [REDACTED]

Email: [REDACTED]
Registration Date: 06/30/2022

48. From July 2022 to June 2023, **Target Account 3** received \$205,299.20 for suspected freelance work in the name of one individual, [REDACTED], from six different software development firms or consulting companies. Based on my training and experience, I know DPRK IT workers often work more jobs than they can handle. They work in teams and all pretend to be one identity, or focus on the top paying jobs and try to remain employed with the other companies as long as possible.

49. The fact that the [REDACTED] alias received six salaries, indicates to me that either multiple people were pretending to be [REDACTED] or just one person was working the top paying jobs while taking a salary and waiting to get fired from the others, which in my training and experience is a common tactic of North Korean IT workers. From July 2022 to June 2023, **Target Account 3** sent \$186,734.00 to two other (previously unknown) Payment Service Provider 1 accounts in China. **Target Account 3** had no bank withdrawals. The money movement between **Target Account 3** and two other Payment Service Provider 1 accounts, particularly those in China, is consistent with **Target Account 3** being used by North Korean IT Workers as a collection point for the funds, which are then transferred to intermediary Payment Service Provider 1 accounts, and then, finally, to a Chinese bank.

50. Payment Service Provider 1 requires the account holders to answer questions to receive payments. **Target Account 3**'s owner (an individual using the alias [REDACTED]) stated that he provided graphic design services through [REDACTED], a freelancing website. However, a review of the documents provided by **Target Account 3**'s owner to Payment Service Provider 1, to comply with know your customer requirements, contained a screenshot of the website:

[REDACTED]/about. This "About Me" page described [REDACTED] work as "provides

business consults, strategy planning, and end-to-end development solutions.” None of these skills are related to “graphic design.” Additionally, invoices provided by **Target Account 3**’s owner to Payment Service Provider 1 listed projects related to software development – not “graphic design” as claimed on [REDACTED].

51. Based on my training and experience, I know that North Korean IT workers will often create fake websites to back stop the false identities they use to obtain jobs. However, because these individuals work in teams and often trade multiple identities, I have observed instances – like the above – where an alias’s advertised skills are inconsistent between different types of media platforms. This occurs because the alias is being used to seek different types of jobs or the IT worker team managing the alias has not properly coordinated that alias’s activities.

52. Also, the website referred to [REDACTED] as a “he,” but the Indonesian identification card used to open the account identified [REDACTED] as a female. North Korean IT workers almost exclusively apply for freelance work using male identification documents, since they are male, but use both male and female aliases when registering their financial accounts. This explains why the [REDACTED] alias was receiving payments to an account owned by the [REDACTED] alias.

53. Additionally, all of the IP addresses after the account was created show that **Target Account 3** was accessed almost exclusively from Singapore, not Indonesia – the purported location of the account holder. The logins were also from different computers (Linux, Windows, Mac), indicating that different individuals were accessing **Target Account 3**. **Target Account 3** was also registered with a US telephone number containing the area code 281, which is for Houston, Texas, another piece of evidence indicating that the owner(s) of the account was

not “[REDACTED]” and likely hiding their identity from the payment service provider.

54. Based on this activity, I submit that probable cause exists to believe that **Target Account 3** was being used by North Korean IT workers to launder the money they obtained from violating IEEPA. Thus, I respectfully submit that there is probable cause to believe that the account contains property, real or personal, which “constitutes or is derived from proceeds traceable” to a “specified unlawful activity.” See 18 U.S.C. § 981(a)(1)(C).

IV. Account Holder ID: 36026036 (Target Account 4)

55. Payment Service Provider 1 Account Holder ID: 36026036 (**Target Account 4**) has an outstanding balance of \$14,999.24 with the following account information:

Name: [REDACTED]
Address: [REDACTED]
Email: [REDACTED]
Registration Date: 03/05/2020

56. From March 2020 to October 2021, **Target Account 4** received \$39,998.00 from [REDACTED], a freelance platform. From June 2022 to June 2023, **Target Account 4** received \$76,135.57 for suspected freelance work in the name of one individual, “[REDACTED]”, from four different companies. Based on my training and experience, I know DPRK IT workers often work more jobs than they can handle. They work in teams and all pretend to be one identity, or focus on the top paying jobs and try to remain employed with the other companies as long as possible.

57. The fact that the [REDACTED] alias received four salaries, indicates to me that either multiple people were pretending to be [REDACTED] or just one person was working the top paying jobs, while taking a salary and waiting to get fired from the others, which in my training and experience is a common tactic of North Korean IT workers.

58. From March 2020 to May 2023, **Target Account 4** sent \$259,196.40 to eleven other Payment Service Provider 1 accounts (at least nine of which were previously unknown) in

China. Two of these accounts were associated with the 387 accounts identified by Payment Service Provider 1. Payment Service Provider 1 records also showed that **Target Account 4** received \$194,553.80 from multiple other Payment Service Provider 1 accounts based in various locations and associated with companies **Target Account 4**'s owner was working for, in addition to the money **Target Account 4** received from other non-Payment Service Provider 1 accounts. **Target Account 4** also had two withdrawals for a total of \$2,530.00 to a bank in Brazil.

59. The money movement and withdrawals are consistent with an account used by North Korean IT workers to launder the proceeds of their criminal violations. If this was normal freelance work, the data would show just one individual with one identity receiving payments from one, maybe two, jobs. Receiving regular payments from multiple employers to one primary account and then distributing those funds to multiple foreign-based accounts, indicates that the owner of that account is trying to hide the proceeds of this activity from the United States.

60. A review of the documents provided by the account holder to open **Target Account 4** identified a Ukrainian passport which appeared to be fraudulent because it contained a low quality image and used inconsistent lettering. Additionally, **Target Account 4**'s owner provided invoices in the name of "[REDACTED]," who purported to be in the United States, rather than supplying invoices in the name of the account holder, [REDACTED].

61. A review of the IP logins for **Target Account 4** showed that the user logged in from IP addresses in multiple countries, which included the United States, China, Japan, Hong Kong, United Kingdom, and Ukraine. However, there was only one successful login in January 2020 from Ukraine, the purported location of **Target Account 4**'s holder. North Korean IT

workers frequently utilize VPNs or proxy services to mask their true location.

62. Based on my training and experience, I believe a VPN or proxy service was used here because there was only one login from the country where the IT worker's alias purportedly claimed to be. All the other IP addresses were observed close-in-time to each other and from multiple countries – indicating multiple logins from different locations or a single VPN or proxy service and one user or more users of that proxy service from the same location. Based on my training and experience this shows that the group either shared a VPN account or they had different accounts at the same VPN provider. The use of IPs at different locations in close proximity, further indicates that the North Korean IT workers running this account were not physically located in the areas that they claimed to be.

63. Based on this activity, I submit that probable cause exists to believe that **Target Account 4** was being used by North Korean IT workers to launder the money they obtained from violating IEEPA. Thus, I respectfully submit that there is probable cause to believe that **Target Account 4** contains property, real or personal, which “constitutes or is derived from proceeds traceable” to a “specified unlawful activity.” *See* [18 U.S.C. § 981\(a\)\(1\)\(C\)](#).

V. Account Holder ID: 56652749 (Target Account 5)

64. Payment Service Provider 1 Account Holder ID: 56652749 (**Target Account 5**) has an outstanding balance of \$9,707.63 with the following account information:

Name: [REDACTED]
Address: [REDACTED]
Email: [REDACTED]@yandex.com
Registration Date: 08/12/2022

65. From December 2022 to May 2023, **Target Account 5** received \$57,120.00 for suspected freelance work in the name of one individual, [REDACTED], from one company. The individual using the alias “[REDACTED]” provided a “Master Services Agreement” to

Payment Service Provider 1 to comply with Payment Service Provider 1's know your customer policies. This agreement was between a company and "[REDACTED]," contained [REDACTED]'s Social Security Number, and associated [REDACTED] with a New Jersey address. I used the Social Security Number to determine if it was real and find who it was associated with. I determined that that the social security number belongs to a [REDACTED] (not [REDACTED]) [REDACTED] who lives in Maine (not New Jersey). Because [REDACTED] does not live in New Jersey and the alias used to register **Target Account 5** had an incorrect middle name, I believe [REDACTED]'s identity has been stolen.

66. From December 2022 to June 2023, **Target Account 5** sent \$76,098.00 to multiple other Payment Service Provider 1 accounts in various countries, with over half of those accounts located in China, and, in addition to the funds received for "[REDACTED]," described above, received \$47,602.63 from multiple accounts in Vietnam, Pakistan, and South Africa. **Target Account 5** was linked to two bank accounts, one in Vietnam and one in China at the [REDACTED]. The [REDACTED] account was also listed on four other Payment Service Provider 1 accounts; those four accounts were owned by individuals who purported to be in Vietnam and Pakistan.

67. Based on my training and experience, it is rare that multiple Payment Service Provider 1 accounts that are allegedly registered in multiple countries with different aliases all use the same [REDACTED] account. When I have observed this pattern in the past, it has been with accounts owned and operated by North Korean IT workers. The use of a single [REDACTED] account for multiple foreign owned accounts at Payment Service Provider 1 and the movement of money between multiple foreign accounts and **Target Account 5** (which was linked to the same [REDACTED] account) indicates that

this activity is linked to North Korean IT worker money laundering.

68. A review of the IP logins for **Target Account 5** identified the user initially created the account from an IP address in Vietnam, the purported location of the account holder. However, all subsequent logins, September 19, 2022, through June 2023 were from the same IP address in Thailand, [REDACTED]. This same IP address has been observed accessing other suspected North Korean IT workers' Payment Service Provider 1 accounts. For example, Payment Service Provider 1 account 53737528 (registered with a Vietnamese IP and identified by Payment Service Provider 1 as part of the 387 accounts) was created from the same IP address on June 14, 2022. Additionally, Payment Service Provider 1 account 31900913 (registered with a Chinese IP and identified as part of the 387 accounts) was accessed from the same IP address from January 20, 2023, to May 23, 2023. Lastly, Payment Service Provider 1 account 61702350 (registered with a Pakistani IP and identified as part of the 387 accounts), was accessed from the same IP address from October 30, 2022, to July 2, 2023.

69. Based on this activity, I submit that probable cause exists to believe that **Target Account 5** was being used by North Korean IT workers to launder the money they obtained from violating IEEPA. Thus, I respectfully submit that there is probable cause to believe that **Target Account 5** contains property, real or personal, which "constitutes or is derived from proceeds traceable" to a "specified unlawful activity." See [18 U.S.C. § 981\(a\)\(1\)\(C\)](#).

VI. Account Holder ID: 44268982 (Target Account 6)

70. Payment Service Provider 1 Account Holder ID: 44268982 (**Target Account 6**) has an outstanding balance of \$8,690.83 with the following account information:

Name: [REDACTED]
Address: [REDACTED]
Email: [REDACTED]
Registration Date: 05/26/2021

71. From July 2021 to December 2023, **Target Account 6** received \$552,480.83 for suspected freelance work performed by [REDACTED] from four different companies and one freelance platform. The fact that the “[REDACTED]” alias received five salaries, indicates to me that either multiple people were pretending to be him or just one person was working the top paying jobs while taking a salary and waiting to get fired from the others, which in my training and experience is a common tactic of North Korean IT workers.

72. From August 2021 to May 2023, **Target Account 6** sent \$550,190.00 to three other Payment Service Provider 1 accounts with most of the transactions being conducted from China and, in addition to the funds received for “[REDACTED],” described above, received \$6,400.00 from two accounts in Nigeria and Pakistan. There were no bank withdrawals on **Target Account 6**. The transactions between these accounts and **Target Account 6** is consistent with how North Korean IT workers launder the proceeds of their freelance activity.

73. If this was normal freelance work, the data would show just one individual with one identity receiving payments from one, maybe two, jobs. Receiving regular payments from multiple employers and foreign accounts and then distributing those funds to multiple foreign-based accounts, indicates that the owner of that account is trying to hide the proceeds of this activity from the United States.

74. Payment Service Provider 1 requires account holders to answer questions in order to receive payments. The account holder for **Target Account 6** stated they were a freelance/contributor on “[REDACTED]”, a website which provides job listings and lists workers available for hire. The account holder provided a URL for a profile on [REDACTED] and used the name “[REDACTED]”. On April 15, 2024, I visited the URL and it listed the name “[REDACTED]”, which is missing the “a” in the last name. The misspelling is an indicator that the

profile at [REDACTED] was created not by the real “[REDACTED]” – who would be unlikely to misspell his name and leave it misspelled – but someone who purported to be him. The creation of accounts at various websites in the name of the owner of the financial account they are using is a common tactic used by North Korean IT workers to make their use of the alias appear legitimate.

75. A review of the IP logins for **Target Account 6** identified the user logged in from IP addresses only in the United States. However, the IP addresses are believed to be associated with a VPN service because a majority of them were part of infrastructure owned by [REDACTED], a hosting provider, and resolved to multiple U.S. cities. None of them were in or near the city of the purported location of the account holder. North Korean IT workers frequently utilize VPNs or proxy services to mask their true location. The change in IP location associated with the logins for **Target Account 6** suggests that this is what was occurring here.

76. **Target Account 6** also used “Nampho” and “Chol” as answers to security questions. These answers are provided by the account holder to reset or login to the account if a password is forgotten. “Nampho” is a city in North Korea and “Chol” is a Korean name.

77. Based on this activity, I submit that probable cause exists to believe that **Target Account 6** was being used by North Korean IT workers to launder the money they obtained from violating IEEPA. Thus, I respectfully submit that there is probable cause to believe that **Target Account 6** contains property, real or personal, which “constitutes or is derived from proceeds traceable” to a “specified unlawful activity.” See [18 U.S.C. § 981\(a\)\(1\)\(C\)](#).

VII. Account Holder ID: 27318468 (Target Account 7)

78. Payment Service Provider 1 Account Holder ID: 27318468 (**Target Account 7**)

has an outstanding balance of \$6,735.70 with the following account information:

Name: [REDACTED]
Address: [REDACTED]
Email: [REDACTED]@163.com
Registration Date: 07/09/2018

79. From August 2018 to January 2019, **Target Account 7** received \$10,047.45 from a freelance platform for suspected freelance work. From September 2021 to May 2023, **Target Account 7** received \$264,658.87 US Dollars (“USD”) and \$453,838.61 Canadian Dollars (“CAD”) in ten different names from various companies for suspected freelance work. From July 2021 to May 2022, the account received \$103,558.45 USD from third party credit cards for suspected freelance work.

80. Based on my training and experience, having ten different names associated with one account, having that account receive payments from several different companies, and having that account receive funds from third party credit cards for other freelance work is consistent with a Payment Service 1 account being used by North Korean IT workers to launder the proceeds of their criminal violations. If this was normal freelance work, the data would show just one individual with one identity receiving payments from one, maybe two, accounts each associated with a different company. Having numerous (likely fake or inaccurate) identities receiving regular payments to one primary bank account from multiple accounts that are associated with many different employers, indicates that the owner of that primary bank account is trying to hide the proceeds of this activity from the United States.

81. From November 2019 to May 2023, **Target Account 7** sent \$796,238.50 to twelve other Payment Service Provider 1 accounts in various countries, with most of the transactions sending funds to five accounts located in China. **Target Account 7** also received \$413,175.32 from multiple accounts, the majority of which appeared to be located in Ukraine.

From August 2018 to April 2023, **Target Account 7** withdrew a total of \$325,700.50 to two Chinese banks: [REDACTED] and the [REDACTED].

82. **Target Account 7** used telephone number +86 [REDACTED] (a Chinese number) and bank account number [REDACTED] (a Bank of China account). Both these identifiers were also used to set up an account at Payment Service Provider 2. Payment Service Provider 2 identified this account and based on an internal investigation concluded it was owned by North Korean IT employees of Yanbian Silverstar. As described above, Yanbian Silverstar is a North Korean front company that coordinates the deployment and revenue generation of IT workers.

83. Based on this activity, I submit that probable cause exists to believe that **Target Account 7** was being used by North Korean IT workers to launder the money they obtained from violating IEEPA. Thus, I respectfully submit that there is probable cause to believe that the account contains property, real or personal, which “constitutes or is derived from proceeds traceable” to a “specified unlawful activity.” See [18 U.S.C. § 981\(a\)\(1\)\(C\)](#).

VIII. Account Holder ID: 46610248 (Target Account 8)

84. Payment Service Provider 1 Account Holder ID: 46610248 (**Target Account 8**) has an outstanding balance of \$6,142.31 with the following account information:

Name: [REDACTED]
Address: [REDACTED]
[REDACTED]
Email: [REDACTED]
Registration Date: 09/06/2021

85. From June 2022 to May 2023, **Target Account 8** received \$23,049.33 from four different companies in nine different names, including “[REDACTED],” described further below, for suspected freelance work. Based on my training and experience, having nine different names

associated with one account, and having that account receive payments from four different companies for those nine other names is consistent with that Payment Service 1 account being used by North Korean IT workers to launder the proceeds of their criminal violations. If this was normal freelance work, the data would show just one individual with one identity receiving payments from one, maybe two, jobs. Having numerous (likely fake or inaccurate) identities receiving regular payments from multiple employers to one primary bank account, indicates that the owner of that account is trying to hide the proceeds of this activity from the United States.

86. From January 2022 to May 2023, **Target Account 8** received \$32,232.15 from third party credit cards for suspected freelance work. From October 2021 to May 2023, **Target Account 8** sent \$59,320.00 to, and received \$11,187.16 from, multiple Payment Service Provider 1 accounts in various countries. **Target Account 8** had two bank accounts listed, one in China (in the name of [REDACTED]) and one in Russia (in the name of [REDACTED]).

87. In February 2024, the FBI received a complaint from a company claiming it was being extorted by a former software developer using the name “[REDACTED]” and the email [REDACTED]. As described above, “[REDACTED]” is one of the names associated with payments received from the four companies that sent salary funds to **Target Account 8**. The company stated that [REDACTED] believed the company was not paying him enough for his work. [REDACTED] demanded \$20,000 and said that if he was not paid, he would post the company’s private code to a public repository. No ransom was paid. Based on my training and experience, I know that North Korean IT workers will – if possible – extort the companies they work for by threatening to post a company’s private code on a public repository. North Korean IT workers usually engage in this tactic to make more money after they are fired.

88. Based on this activity, I submit that probable cause exists to believe that **Target**

Account 8 was being used by North Korean IT workers to launder the money they obtained from violating IEEPA. Thus, I respectfully submit that there is probable cause to believe that **Target Account 8** contains property, real or personal, which “constitutes or is derived from proceeds traceable” to a “specified unlawful activity.” See [18 U.S.C. § 981\(a\)\(1\)\(C\)](#).

IX. Account Holder ID: 56097094 (Target Account 9)

89. Payment Service Provider 1 Account Holder ID: 56097094 (**Target Account 9**) has an outstanding balance of \$5,681.00 with the following account information:

Name: [REDACTED]
Address: [REDACTED]
[REDACTED]
Email: [REDACTED]@sina.com
Registration Date: 07/28/2022

90. From September 2022 to May 2023, **Target Account 9** received \$3,875.00 from Wise, formerly TransferWise, an online money transfer service, for suspected freelance work conducted by the alias “[REDACTED]”. From January 2023 to May 2023, **Target Account 9** received \$13,854.27 from companies that I suspect employed [REDACTED]. From January 2023 to May 2023, **Target Account 9** sent \$3,958.00 to, and received \$44,648.16 from, multiple Payment Service Provider 1 accounts in various countries including China.

91. The money movement and withdrawals are consistent with an account used by North Korean IT workers to launder the proceeds of their criminal violations. Receiving regular payments from multiple employers to one primary account and then distributing those funds to multiple foreign-based accounts, indicates that the owner of that account is trying to hide the proceeds of this activity from the United States.

92. A review of the documents provided by **Target Account 9**’s owner for account verification revealed two similar invoices were submitted for a work contract. One had the name

“[REDACTED]”, email address [REDACTED]@sina.com, and the other had the name “[REDACTED]”, email address [REDACTED]@sina.com. According to the metadata for both invoices, they were created by “[REDACTED]”. The name discrepancy between the invoices and the fact that they were both created by a third person with a different name is a common mistake for North Korean IT worker accounts because they use multiple identities for different freelance work. In this case it appears the account holder inadvertently submitted an invoice for a different identity than the alias used to register **Target Account 9**.

93. In November 2023, a foreign government partner who in the past has provided reliable information about North Korean IT workers, that the FBI has been able to corroborate, provided a list of payment accounts used by North Korean IT workers. The list included **Target Account 9**, which was registered with the email address [REDACTED]@sina.com as well as an account registered with the email address [REDACTED]@sina.com. As described above, these two email accounts appeared in the submitted invoices for **Target Account 9**.

94. Based on this activity, I submit that probable cause exists to believe that **Target Account 9** was being used by North Korean IT workers to launder the money they obtained from violating IEEPA. Thus, I respectfully submit that there is probable cause to believe that the account contains property, real or personal, which “constitutes or is derived from proceeds traceable” to a “specified unlawful activity.” See [18 U.S.C. § 981\(a\)\(1\)\(C\)](#).

SEIZURE PROCEDURE FOR TARGET ACCOUNTS

95. The foregoing establishes probable cause to believe that the funds held in the **Target Accounts** are subject to civil and criminal forfeiture because those accounts and the funds within them were obtained through illegal employment by North Korean IT Workers in violation of U.S. sanctions, and were involved in a money laundering conspiracy.

96. Should this seizure warrant be granted, law enforcement intends to work with Payment Service Provider 1 to seize the funds contained within the **Target Accounts** by transferring the funds to a U.S. government-controlled account.



97. The seized currency in the **Target Accounts** will remain at the government-controlled account pending transfer of all right, title, and interest in the forfeitable property in the **Target Accounts** to the United States upon completion of forfeiture proceedings, to ensure that access to or manipulation of the forfeitable property cannot be made absent court order or, if forfeited to the United States, without prior consultation by the United States.

CONCLUSION

98. Based on the information contained herein and my training and experience, I submit that the **Target Accounts** are subject to seizure and forfeiture, pursuant to the above-referenced statutes. Based on the foregoing, I request that the Court issue the proposed seizure warrant.

99. Because Attachment A will be served on Payment Service Provider 1, which currently holds the associated funds, and thereafter, at a time convenient to it, will transfer the funds to the U.S. government, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

I declare under the penalty of perjury that the foregoing is true and correct to the best of my knowledge.



Special Agent
Federal Bureau of Investigation

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to
Federal Rules of Criminal Procedure 4.1 and 41 on this 18th day of July, 2024.



HONORABLE JOHN M. BODENHAUSEN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
PROPERTY TO BE SEIZED

Pursuant to this warrant, federal law enforcement agents are authorized to effectuate the seizure of all money, funds, and financial instruments deposited or credited to the below identified properties (collectively, the “**Target Accounts**”) by serving this warrant on [REDACTED]:

	Account Holder ID	Email	Registration Date	Amount USD
Target Account 1	39566449	[REDACTED]@163.com	08/22/2020	\$239,927.62
Target Account 2	51679820	[REDACTED]	04/07/2022	\$136,604.68
Target Account 3	54302706	[REDACTED]	06/30/2022	\$16,537.21
Target Account 4	36026036	[REDACTED]	03/05/2020	\$14,999.24
Target Account 5	56652749	[REDACTED]@yandex.com	08/12/2022	\$9,509.43
Target Account 6	44268982	[REDACTED]	05/26/2021	\$8,690.83
Target Account 7	27318468	[REDACTED]@163.com	07/09/2018	\$6,735.70
Target Account 8	46610248	[REDACTED]	09/06/2021	\$6,142.31
Target Account 9	56097094	[REDACTED]@sina.com	07/28/2022	\$5,681.00
Total				\$444,828.01