UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Seizure of

Approximately $1,134,350.67 held in [redacted] accounts, further described in Attachment A

Case No. 4:22MJ1298 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

Approximately $1,134,350.67 held in [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

October 25, 2022
Date and Time Issued

at St. Louis, Missouri
City and State

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

[redacted]

Signature of Judicial Officer

AFFIDAVIT IN SUPPORT AN APPLICATION FOR 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 $1,134,350.67 held in the specific [redacted] accounts listed in Attachment A (the "**Target Accounts**"). [redacted] is a U.S.-based financial services company that provides online money transfer and digital payment services to its customers, who can use their [redacted] account to receive, store, and send money, including to counterparties from outside of the [redacted] 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") 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. There is probable cause to seize the funds in the **Target Accounts** as proceeds traceable to IEEPA violations, and as property involved in money laundering violations, or traceable to such property.

APPLICABLE STATUTES

A. International Emergency Economic Powers Act (IEEPA)

5. Under IEEPA, it is a crime to willfully violate or conspire to violate any license, order, regulation, or prohibition issued pursuant to IEEPA, including restrictions imposed by the Department of Treasury. 50 U.S.C. § 1705(a).

6. The Department of Treasury's Office of Foreign Asset Control (OFAC) has the authority to designate for sanctions entities or people determined to have violated the President's Executive Orders.

7. On September 13, 2018, OFAC designated for sanctions a North Korean information technology firm based in China named Yanbian Silverstar Network Technology Co., Ltd ("Yanbian Silverstar"), as well its Russia-based front company, Volasys Silver Star, for violating the President's Executive Orders. These entities exported workers from North Korea to generate revenue for the Government of North Korea (in violation of Executive Order 13722), and employed North Korean workers in the information technology industry (in violation of Executive Order 13810). The same OFAC designation also included a North Korean national, [redacted], identified by OFAC as the CEO of Yanbian Silverstar and Volasys Silver Star.

8. According to the OFAC designation press release, the sanctioned parties had 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, 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.

B. Money Laundering

9. 18 U.S.C. § 1956(h) criminalizes a conspiracy to commit money laundering.

10. 18 U.S.C. § 1956(a)(1)(B)(i) criminalizes conducting, or attempting to conduct, a financial transaction which involves the proceeds of specified unlawful activity, knowing that the property involved in such financial transaction represents the proceeds of some form of unlawful activity, and knowing that the transactions were designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of said specified unlawful activity.

11. Under 18 U.S.C. § 1956(c)(7)(D), the term "specified unlawful activity" includes violations of IEEPA. The financial transactions described in this affidavit are overt acts in furtherance of a money laundering conspiracy to conceal IEEPA violations.

C. Forfeiture

12. Pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c), any property which constitutes or is derived from proceeds traceable to a violation of IEEPA, is subject to criminal and civil forfeiture.

13. Property involved in a money laundering offense is subject to forfeiture under both civil and criminal forfeiture authorities. Pursuant to 18 U.S.C. § 981(a)(1)(A), any property, real or personal, involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956, or any property traceable to such property, is subject to civil forfeiture. In addition, pursuant to 18 U.S.C. § 982(a)(1), any property involved in a violation of 18 U.S.C. § 1956, or any property traceable to such property, is subject to criminal forfeiture. Forfeiture pursuant to these statutes applies to more than just the proceeds of the crime. These forfeitures encompass all property "involved in" the crime, which can include untainted funds that are comingled with tainted funds derived from illicit sources.

14. Pursuant to 18 U.S.C. § 981(b), property subject to civil forfeiture may be seized by a civil seizure 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). As detailed below, acts in furtherance of the fraud and money laundering scheme under investigation occurred in the Eastern District of Missouri. The criminal forfeiture statute, 18 U.S.C. § 982(b)(1), incorporates the procedures in 21 U.S.C. § 853, which provides authority for the issuance of a seizure warrant for property subject to criminal forfeiture.

15. 18 U.S.C. § 984 allows the United States to seize for civil forfeiture identical substitute property found in the same place where the "guilty" property had been kept. For purposes of Section 984, this affidavit need not demonstrate that the funds now in the **Target Accounts** are the particular funds involved in the fraud and money laundering violations, so long

as the forfeiture is sought for other funds on deposit in that same account. Section 984 applies to civil forfeiture actions commenced within one year from the date of the offense.

16. Based on the foregoing, the issuance of this seizure warrant is authorized under 21 U.S.C. § 853(f) and 18 U.S.C. § 982(b)(1) for criminal forfeiture; and 18 U.S.C. §§ 981(b) and 984 for civil forfeiture. Notwithstanding the provisions of Rule 41(a) of the Federal Rules of Criminal Procedure, the issuance of this seizure warrant in this district is appropriate under 18 U.S.C. § 981(b)(3) and 28 U.S.C. § 1355(b)(1) because acts or omissions giving rise to the forfeiture occurred in the Eastern District of Missouri.

BACKGROUND REGARDING NORTH KOREAN INFORMATION TECHNOLOGY WORKERS

17. According to a May 16, 2022, report jointly issued by the U.S. Department of State, Department of 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.

18. Because this work violates U.S. sanctions, 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.

19. 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.

20. 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.

21. The North Korean IT workers are primarily 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 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 appear that they are connecting to online services from false locations.

FACTS ESTABLISHING PROBABLE CAUSE TO BELIEVE CRIMES HAVE BEEN COMMITTED

22. In August 2019, the FBI interviewed an individual located in the United States ("Individual 1") who had an account at [redacted] is a global freelancing platform based in the United States, which serves as an online marketplace where businesses advertise for independent professionals or freelance workers, who in turn can find work in a variety of industries, including software development and information technology.

23. Individual 1 described communications with another individual who has been using the [redacted] account [redacted] and the telephone number [redacted] This second individual is referred to as [redacted]

24. Individual 1 allowed [redacted] to use Individual 1's [redacted] account for freelance work. Individual 1 also agreed to purchase a laptop for [redacted] and keep it in Individual 1's home in the United States. Individual 1 told the FBI that [redacted] used remote access software to use the computer located in Individual 1's residence, and that the computer's monitor showed that the remote user was using the computer for [redacted] Individual 1 eventually had four laptops used by [redacted] with [redacted] paying Individual 1 $100

per month per laptop.

25. [redacted] also requested that Individual 1 find other people with additional [redacted] accounts that [redacted] could use, but Individual 1 did not refer any people to [redacted].

26. For the work completed by [redacted] through Individual 1's [redacted] account, the payments would be channeled through Individual 1's [redacted] account and sent (minus a portion of the money kept by Individual 1) to [redacted] using his accounts at the payment platforms [redacted] and [redacted].

27. According to Microsoft, the [redacted] account [redacted] used by Individual 1 to contact [redacted] was registered with the email address [redacted]@yandex.com. Yandex.com is a Russian email provider.

28. According to [redacted] the account registered with the telephone number [redacted]-[redacted] used by Individual 1 to contact [redacted] was registered using the email address [redacted]@gmail.com, and the answer to the security question is "[redacted]."

29. According to [redacted] the account used by [redacted] to receive payment from Individual 1 for freelance work was registered using the email address [redacted]@126.com (126.com is a Chinese email provider), and the answer to the security question was "yinxing," which is Chinese for Silver Star. According to [redacted] this account used by [redacted] to receive payment from Individual 1 for freelance work received over $85,000 between April 2018 and October 2019.

30. Based on my training and experience, the use of a Chinese email provider and security question, the similarity of the security question to the name of the sanctioned North Korean IT worker front company Yanbian Silverstar, the receipt of funds, and the use of an

intermediary's [redacted] account, multiple [redacted] accounts, multiple email accounts, and a U.S.-based laptop to conduct freelance IT work, I have probable cause to believe that [redacted] is a North Korean IT worker living in China and working at Yanbian Silverstar.

31. Through an approved undercover operation, the FBI utilized an online undercover employee ("OCE") to communicate while in the Eastern District of Missouri via [redacted] with [redacted] In August 2020, [redacted] explained his need for a U.S. [redacted] account and that he would pay 15% of the monthly earnings to the OCE for the use of the account. Also, [redacted] needed a laptop so he could connect via a remote desktop-type application. This would provide [redacted] with the appearance of residing in the United States and the ability to avoid using a Virtual Private Network ("VPN") IP address which might be blocked by [redacted] On August 16, 2020, [redacted] agreed to provide $75 to the OCE to purchase a laptop. On August 17, 2020, OCE received the $75 payment from a [redacted] account registered with email address [redacted]@126.com.

32. According to [redacted] the account used by [redacted] to receive payment from Individual 1 for freelance work logged on from IP address 36.97.143.26 ("IP Address 1") from April 27, 2018, to October 13, 2019. Based on databases regularly relied upon by the FBI, IP Address 1 resolves to China Telecom, Jilin, China and was associated with a dedicated server during this time period. This means accounts accessed by IP Address 1 during this time period would have been working together, likely from the same location and for the same organization. As described below, records from [redacted] multiple accounts accessed from IP Address 1 were used by Yanbian Silverstar freelancers.

33. Based on my training and experience, and evidence of a North Korean IT worker living in China and working at Yanbian Silverstar using a Chinese dedicated server located at IP

Address 1 to access [redacted] I have probable cause to believe that others using IP Address 1 between April 27, 2018, to October 13, 2019, are also North Korean IT workers living in China and working at Yanbian Silverstar.

34. According to [redacted] there were 64 [redacted] accounts that were created or accessed from IP Address 1 between April 27, 2018, to October 13, 2019. Many contained the name "Silver Star" in their subscriber information and indicated that the users' location was in Jilin, China, corroborating that the accounts are used by North Korean IT workers living in China and working at Yanbian Silverstar. For example, one of these [redacted] accounts listed the business name "Yanbian Silver Star Network Technology Co., Ltd.," and an address in Jilin, China.

35. The FBI's review of the account information for these [redacted] accounts showed payments from freelancer platforms such as [redacted]. Many [redacted] accounts also listed multiple email addresses in their subscriber information (allowing the user to register numerous freelancer platform accounts with the same [redacted] account). These characteristics corroborate the probable cause that these accounts are used by North Korean IT workers living in China and working at Yanbian Silverstar.

36. In February and July, 2022, United States Magistrate Judges Shirley P. Mensah and John M. Bodenhausen in the Eastern District of Missouri signed federal search warrants for numerous Google and Microsoft for accounts associated to Yanbian Silverstar actors based on the information received from [redacted] The communications from these Google and Microsoft accounts discussed using identities of third parties 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.

37. A review of the records from the Google and Microsoft search warrants identified additional email accounts, bank accounts, telephone numbers, fictitious company names, and stolen personally identifiable information (PII), such as SSN, date of birth, and address, used by the Yanbian Silverstar actors to create their online payment and freelancer platform accounts.

38. The email addresses and financial identifiers associated with Yanbian Silverstar, provided by [redacted] Microsoft, and Google, were in turn provided to [redacted] provided a list of accounts matching those identifiers. The general pattern of these accounts includes physical addresses in China, payments received from freelancer and payment platforms, and withdrawals of funds to accounts at Chinese banks. I know from my training and experience that North Korean IT workers frequently use China-based banks to spend their freelancer revenue or else transmit it to North Korea.

39. The FBI conducted analysis of the accounts provided by [redacted] and a subset of those accounts are the funds in the **Target Accounts** to be seized in Attachment A.

40. The below 26 accounts, identified by [redacted] Cardholder ID, total $806,517.12 in proceeds from the fraud scheme and are further described below. These are the accounts which had a remaining balance as of the date of this application and were identified by the FBI as being used by Yanbian Silverstar and Volasys Silver Star. The subscriber information listed for each account was provided by the subscriber to [redacted]

a. [redacted] Cardholder ID: 32787138 had an outstanding balance of $230,451.28 with the following account information:

Name: [redacted]

Registration Date: 7/12/2019

i. During the period of June 2020 to April 2022, the account received

$1,458,952.22 from other [redacted] accounts, sent $259,405.39 to other [redacted] accounts, and withdrew a total of $969,100.00 to a bank account in China.

ii. According to [redacted] records, the email address [redacted]@126.com was also used for the [redacted] account that paid an internet service provider (Bluehost) to host the domain "Silverstarchina.com." Silverstarchina.com was the public website for the sanctioned China-based front company Yanbian Silverstar. This corroborates that the person controlling this email address is a sanctioned North Korean IT worker.

b. [redacted] Cardholder ID: 32823195 had an outstanding balance of $79,400.84 with the following account information:

Name: [redacted]
Registration Date: 7/15/2019

i. During the period of July 2019 to March 2022, the account received $190,500.00 in payments from [redacted] received $57,210.50 in payments from [redacted] received $1,756,978.95 from other [redacted] accounts, sent $494,674.52 to other [redacted] accounts, and withdrew a total of $1,469,883.96 to a bank account in China.

ii. According to records from [redacted] [redacted]@126.com was also an email account for a [redacted] account used to pay the internet service provider (Bluehost) to host the domain "Silverstarchina.com," the public website for the sanctioned China-based front company Yanbian Silverstar.

c. [redacted] Cardholder ID: 26364278 had an outstanding balance of $75,054.35 with the following account information:

Name: [redacted]
Registration Date: 4/27/2018

i. During the period of May 2018 to March 2022, this [redacted] received $324,629.03 in payments from [redacted] (freelance employment platform), received $1,533,094.84 from other [redacted] accounts, sent $1,328,543.13 to other [redacted] accounts, and withdrew $475,000 to a bank account in China.

ii. The email account [redacted]@126.com was used to register a [redacted] account which sent two payments ($50 on 3/15/2018 and $225 on 3/26/2018) to Individual 1 for the use of the laptop on their home. According to [redacted] records, the [redacted]@126.com [redacted] account also received a total of $115,983.48.

iii. According to records from Microsoft, [redacted] used the [redacted] account [redacted] to tell another North Korean IT Worker, using the [redacted] account [redacted], that he had withdrawn $2,186 from [redacted]@126.com.

iv. The laptop that [redacted] rented from the FBI OCE was recorded logging in to a [redacted] account (registered using the email address [redacted]@gmail.com) in September 2020, and that [redacted] account showed three transactions totaling $400 to [redacted]@126.com. According to records from Google, the recovery address for the google

account [redacted]@gmail.com was [redacted]'s email address [redacted]@gmail.com. Based on my training and experience, I know that North Korean IT workers frequently pay accounts they control in order to move money between accounts to mask the origin and destination of funds from freelance IT work.

d. [redacted] Cardholder ID: 27361057 had an outstanding balance of $73,258.78 with the following account information:

Name: [redacted]
Registration Date: 7/12/2018

i. The email address' use of "eden" followed by three letters is similar [redacted]@126.com, the email account used to register [redacted] account, which he used to receive freelance payment funds from Individual 1.

ii. The email account [redacted]@126.com was used to register a [redacted] account which sent one payment for $265 on 6/17/2018 to Individual 1 for the use of laptops in their home, confirming that the email address is controlled by Yanbian Silverstar North Korean IT workers. According to [redacted] records this [redacted] account logged in from IP Address 36.97.143.26, the Yanbian Silverstar dedicated server, and received a total of $601,430.97.

iii. During the period of July 2018 to March 2022, this [redacted] account received $800,213.26 in payments from [redacted] received $1,824,810.82 from other [redacted] accounts, sent $502,164.80 to other [redacted]

accounts, and withdrew a total of $2,084,655.76 to a bank account in China.

e. [redacted] Cardholder ID: 27738625 had an outstanding balance of $45,934.74 with the following account information:

Name: [redacted]
Registration Date: 7/12/2018

i. This [redacted] account received $102,000 from the [redacted] account controlled by [redacted]@126.com, which was a [redacted] account used to pay Individual 1 for the use of the laptop in their home.

ii. The account's email address "[redacted] is similar to the name of the front company Yanbian Silverstar.

iii. During the period of October 2018 to March 2022, this [redacted] account received $67,000 in payments from [redacted] received $3,254,424.93 from other [redacted] accounts, sent $311,799.47 to other [redacted] accounts, and withdrew a total of $2,979,851.59 to a bank account in China.

f. [redacted] Cardholder ID: 41482927 had an outstanding balance of $36,413.40 with the following account information:

Name: [redacted]
Registration Date: 12/14/2020

i. The [redacted] account registered with email address [redacted]@126.com was identified as sending $800 on February 3, 2021, to the [redacted] account registered with email address

[redacted]@yahoo.com. Email address [redacted]@yahoo.com is the recovery address for [redacted]@yahoo.com, which was accessed by the remote user of the computer at the home of Individual 1.

ii. According to [redacted] records from Microsoft, in 2020, the [redacted] user live:[redacted] discussed IT work with [redacted] including worker schedules, account creation, interviewing for freelance IT work, and payments for freelance IT work.

iii. According to [redacted] records from Microsoft, in 2021, the email address [redacted]@126.com was repeatedly sent from the [redacted] user [redacted] to the [redacted] user [redacted] (the [redacted] username of the Company President, [redacted]), in Korean-language [redacted] Based on the content and context of these [redacted] there is probable cause to believe the user of the email address [redacted]@126.com is a North Korean IT worker.

g. [redacted] Cardholder ID: 33072116 had an outstanding balance of $33,190.57 with the following account information:

Name: [redacted]
Registration Date: 8/2/2019

i. According to [redacted] records from Microsoft, in 2018, [redacted] user [redacted] had multiple [redacted] conversations with [redacted] about coordinating North Korean IT work. In 2020, [redacted] user [redacted] sent the email address [redacted]@126.com alongside a dollar amount as part of a discussion about payments for freelance IT work. Based on this, I

have probable cause to believe that the [redacted] account associated with [redacted]@126.com is used by North Korean IT workers.

h. [redacted] Cardholder ID: 27851354 had an outstanding balance of $27,810.94 with the following account information:

Name: [redacted]
Registration Date: 8/15/2018

i. The email address use of "eden" followed by three letters is similar to [redacted]@126.com, the email account used to register [redacted] account, which he used to receive payment from Individual 1 for freelance work.

ii. According to [redacted] records from Microsoft, in 2020, the [redacted] user [redacted] discussed IT work with [redacted] including worker schedules, account creation, interviewing for freelance IT work, and payments for freelance IT work. In 2019, another [redacted] user repeatedly sent the [redacted] user [redacted] the email address [redacted]@126.com, once alongside the number 2500. Based on this, I have probable cause to believe that the user of the email address [redacted]@126.com is involved in collecting payments for North Korean IT work.

i. [redacted] Cardholder ID: 43552963 had an outstanding balance of $25,134.92 with the following account information:

Name: [redacted]

Registration Date: 4/20/2021

i. On July 3, 2021, while using the FBI monitored laptop, a North Korean IT worker logged in to a [redacted] account using stolen PII of a real person, and attempted to send $1,300 to the [redacted] account with the email address [redacted]@126.com, but the transaction failed.

ii. On July 5, 2021, while using the FBI monitored laptop, a North Korean IT worker logged in to a [redacted] account and sent $150 to the email address [redacted]@126.com for "web design." Based on my training and experience, I know that the sending of smaller amounts to other North Korean controlled accounts helps to mask the source of the funds and ensure the payments are not flagged by [redacted]

j. [redacted] Cardholder ID: 41509922 had an outstanding balance of $24,976.32 with the following account information:

Name: [redacted]

Registration Date: 12/15/2020

i. On July 3, 2021, while using the FBI monitored laptop, a North Korean IT worker logged in to a [redacted] account in the name of an individual who's PII was stolen, and made three attempts to send more than $1,000 to the [redacted] account with the email address [redacted]@163.com, but each transaction failed.

ii. In 2020, according to [redacted] records from Microsoft, [redacted] corresponded in Korean via [redacted] about IT projects with the [redacted]

account registered with the email address [redacted]@gmail.com. According to records from Google, [redacted]@gmail.com accessed North Korea maps and a North Korean news site, the email account was used to apply for IT worker jobs, and the cloud storage contained resumes, job descriptions, interview scripts, and spreadsheets in Korean cataloging monthly revenue of various email addresses. According to records from Slack, the user with the email address [redacted]@gmail.com also operated the channel [redacted]slack.com, which catalogued numerous entries described as "weekly payments for app development" to the [redacted] account [redacted]@163.com. This corroborates that the email address [redacted]@163.com is used for North Korean IT work.

k. [redacted] Cardholder ID: 43476624 had an outstanding balance of $22,972.28 with the following account information:

Name: [redacted]
Registration Date: 4/16/2021

i. According to [redacted] records from Microsoft, in 2017, the [redacted] user [redacted] discussed IT work with [redacted] including worker schedules, creating and logging into remote accounts, purchasing virtual private servers, and emails with employers for freelance IT work.

ii. According to [redacted] records from Microsoft, in 2021 the email address [redacted]@126.com was repeatedly sent by the user [redacted] alongside a dollar amount, in Korean-language [redacted]

[redacted] Based on the content and context of these [redacted] there is probable cause to believe the email address [redacted]@126.com is controlled and used by the user of [redacted] for freelance IT work.

l. [redacted] Cardholder ID: 33012110 had an outstanding balance of $19,128.39 with the following account information:

Name: [redacted]
Registration Date: 7/29/2019

i. According to records from [redacted], on June 22, 2020, the [redacted] account with the email address [redacted]@126.com paid $30 to an individual known to provide false identification documents to North Korean IT workers.

ii. Corroborating the probable cause that [redacted]@126.com is a North Korean IT worker, the [redacted] account registered with that email account was also registered with other email addresses whose usernames included the name [redacted] Additionally, notes included from various payments to that [redacted] account indicated the payment was for IT development work.

m. [redacted] Cardholder ID: 32820879 had an outstanding balance of $18,776.61 with the following account information:

Name: [redacted]
Registration Date: 7/14/2019

i. According to [redacted] records from Microsoft, in 2020, the [redacted] users [redacted] discussed IT work with [redacted]

ii. According to [redacted] records from Microsoft, in 2021 the email address [redacted]@126.com was repeatedly sent by the [redacted] user [redacted] to the [redacted] user [redacted] alongside a dollar amount, in Korean-language [redacted] Based on the content and context of these [redacted] there is probable cause to believe the user of the email address [redacted]@126.com is a North Korean coordinating with the user of [redacted] for freelance IT work.

n. [redacted] Cardholder ID: 28661935 had an outstanding balance of $14,111.60 with the following account information:

Name: [redacted]
Registration Date: 10/14/2018

i. According to [redacted] records from Microsoft, in 2020, the [redacted] user [redacted] discussed IT work with [redacted] including worker schedules, account creation, interviewing for freelance IT work, and payments for freelance IT work.

ii. According to [redacted] records from Microsoft, in 2021, the email address [redacted]@126.com was repeatedly sent by the [redacted] user [redacted] (the [redacted] username of Yanbian Silverstar Company President [redacted]) to the [redacted] user [redacted], alongside a dollar amount, in Korean-language [redacted] Based on the content and

context of these [redacted] there is probable cause to believe the user of the email address [redacted]@126.com is a North Korean coordinating freelance IT work.

o. [redacted] Cardholder ID: 32775158 had an outstanding balance of $9,361.25 with the following account information:

Name: [redacted]
Registration Date: 7/11/2019

i. According to [redacted] records from Microsoft, in 2019, [redacted] explained that he used the '[redacted]' [redacted] account to spend $1,300 on expenses related to North Korean IT work. In a 2020 [redacted] conversation about purchasing laptops for IT work, [redacted] provided the email address [redacted]@126.com. There is therefore probable cause to believe that the user of [redacted]@126.com is a North Korean IT worker.

ii. The email address [redacted]@126.com was used to log into [redacted] from IP Address 1, indicating that the user has access to the Yanbian Silverstar dedicated server, and corroborating that the user of this email account is a North Korean IT worker.

p. [redacted] Cardholder ID: 32006723 had an outstanding balance of $7,245.00 with the following account information:

Name: [redacted]
Registration Date: 5/13/2019

i. According to [redacted] records from Microsoft, in 2020, the [redacted] user [redacted] discussed IT work with [redacted] worker schedules, account creation, interviewing for freelance IT work, and payments for freelance IT work. According to [redacted] records from Microsoft, in 2017 and 2019, the email address [redacted]@126.com was sent from the [redacted] user [redacted] to the [redacted] user [redacted] (the [redacted] username of Yanbian Silverstar Company President [redacted], in Korean-language [redacted]. In 2019 the message included a dollar amount. Based on the content and context of these [redacted] there is probable cause to believe the user of the email address [redacted]@126.com is a North Korean coordinating freelance IT work.

ii. The [redacted] account with the email address [redacted]@126.com logged into [redacted] from IP Address 1, indicating that the user has access to the Yanbian Silverstar dedicated server. The email address also contains the word "Silverstar" and received funds from the [redacted] account [redacted]@gmail.com, corroborating that the user of this email account is a North Korean IT worker.

q. [redacted] Cardholder ID: 40923961 had an outstanding balance of $6,115.55 with the following account information:

Name: [redacted]

Registration Date: 11/9/2020

i. According to records received from [redacted] the email address [redacted]@gmail.com was registered as one of the email addresses for a [redacted] account that sent funds to pay for the internet domain Silverstarchina.com, the public website used by Yanbian Silverstar to advertise their freelancer services.

ii. According to records received from [redacted] the account registered with the email address [redacted]@gmail.com included as security answers the Korean names [redacted], corroborating that this account is controlled by a Yanbian Silverstar North Korean IT worker, despite its registered address in Texas.

r. [redacted] Cardholder ID: 33056635 had an outstanding balance of $6,071.58 with the following account information:

Name: [redacted]
Registration Date: 8/1/2019

i. According to records received from [redacted], on August 17, 2020, the [redacted] account with the email address [redacted]@126.com was used by [redacted] to pay $75 towards the purchase of a laptop to conduct IT work from the home of a FBI online undercover employee located in the United States. Based on FBI monitoring of this laptop, North Korean IT workers connected to this laptop via a remote desktop application, and then connected to freelance platforms, creating the appearance of logging in from the United States. Based on my training and experience there is

probable cause to believe that the user of this email address is a North Korean IT worker.

ii. According to [redacted] records from Microsoft, on August 31, 2020, the email address [redacted]@126.com was sent to [redacted] in Korean-language [redacted] alongside dollar amounts and notes about completed projects. Based on my training and experience, this corroborates that the user of the email address [redacted]@126.com is a North Korean IT worker.

s. [redacted] Cardholder ID: 32016016 had an outstanding balance of $3,743.36 with the following account information:

Name: [redacted]
Registration Date: 5/14/2019

i. According to records from [redacted] the account with the email address [redacted]@126.com logged in from IP Address 1, indicating that the user has access to the Yanbian Silverstar dedicated server.

ii. The [redacted]@126.com [redacted] account was also registered using the email address [redacted]@yahoo.com, the name of the sanctioned China-based front company Yanbian Silverstar, and received funds from the account using the email address [redacted]@126.com (also similar to the name of Yanbian Silverstar), corroborating that the user of this email account is a North Korean IT worker associated with and transacting with Yanbian Silverstar.

t. [redacted] Cardholder ID: 33145450 had an outstanding balance of $3,368.60 with the following account information:

Name: [redacted]
Registration Date: 8/7/2019

i. A review of the [redacted] records for this account revealed a Russian telephone number but an address in China that is the same or nearly the same as those used by numerous other Yanbian Silverstar IT workers in their [redacted] registrations.

ii. The name [redacted] identified a [redacted] account using the email address [redacted]@126.com and the same address as the [redacted] account. The [redacted] account listed 9 additional email addresses, all in different names. Based on my experience and investigation, I know that North Korean IT workers utilize different personas with different email addresses, and add those email addresses to their [redacted] account so that the same [redacted] account can be used for multiple personas.

u. [redacted] Cardholder ID: 33352633 had an outstanding balance of $2,711.49 with the following account information:

Name [redacted]
Registration Date: 8/23/2019

i. [redacted] records revealed that the email address [redacted]@gmail.com shared a [redacted] account with the email address [redacted]@gmail.com. Records from Google revealed that the

email address [redacted]@gmail.com was registered using the recovery address [redacted]@gmail.com. This is the email address associated with the [redacted] address registered using the telephone number that [redacted] used to communicate with Individual 1. Records from [redacted] revealed that the telephone number used by [redacted] to communicate with Individual 1 was used to register a [redacted] account with the email address [redacted]@gmail.com.

ii. The [redacted] account with the email address [redacted]@gmail.com logged in to [redacted] from IP Address 1, indicating that the user has access to the Yanbian Silverstar dedicated server. The email address [redacted]@gmail.com also shared a [redacted] account with the email address [redacted]@126.com (with the name [redacted] and an address in China), corroborating that the user of this email account is a North Korean IT worker working for Yanbian Silverstar.

v. [redacted] Cardholder ID: 45177501 had an outstanding balance of $1,739.80 with the following account information:

Name: [redacted]
Registration Date: 7/1/2021

i. Google records revealed the email address [redacted]@gmail.com was linked by cookies (meaning that it was accessed using the same device and browser) to [redacted]@gmail.com. Google records revealed that [redacted]@gmail.com uses the recovery email address

[redacted]@gmail.com (which is an email address used to register the [redacted] account used by [redacted]

ii. [redacted] records for the email address [redacted]@gmail.com identified the account used the security answer [redacted]. The use of eden120 as the answer to the security question for this [redacted] account, as well as for the [redacted] account controlled by [redacted] corroborates that this account is controlled by Yanbian Silverstar North Korean IT workers.

w. [redacted] Cardholder ID: 28739311 had an outstanding balance of $1,447.26 with the following account information:

Name: [redacted]
Registration Date: 10/19/2018

i. There is probable cause to believe that the [redacted] account registered using the email address [redacted]@126.com is controlled by Yanbian Silverstar North Korean IT workers because it follows the same naming convention of three letters with the word "eden," as other email addresses used by [redacted] and because the mailing address used to register the [redacted] account is the same as the mailing address used to register another [redacted] account of another North Korean IT worker ([redacted]@126.com) who used that account to pay for the Silverstarchina.com domain, the website for Yanbian Silverstar.

x. [redacted] Cardholder ID: 42779276 had an outstanding balance of $1,292.79 with the following account information:

Name: [redacted]
Registration Date: 3/4/2021

i. Google search warrant records for a different email account, [redacted]@gmail.com (which was used to register a [redacted] account which [redacted] with [redacted] account about North Korean IT work), revealed a Google drive filled with multiple videos, scripts, resumes, and job descriptions to obtain freelancer jobs. The Google drive also contained an excel-type sheet containing monthly deposits and withdrawals for IT worker payments accounts, and a spreadsheet containing stolen Personal Identifiable Information (PII) including names, dates of birth, social security numbers, and addresses. The list contained the PII for [redacted].

ii. Slack records identified [redacted] in which the same stolen name, address, and email address were shared from the user, [redacted]. These [redacted] occurred in Korean.

iii. The [redacted] account registered using this stolen identity sent over $153,474.57 to various [redacted]ccounts in China, Ukraine, Pakistan, and India, including payments totaling $39,906 from December 24, 2021 to March 29, 2022, to another [redacted] Cardholder ID ([redacted]), registered using the email address [redacted]@126.com, which was also listed on the excel-type sheet of IT workers and their monthly payments. There is therefore probable cause to believe that this email account is used by a North Korean IT worker.

y. [redacted] Cardholder ID: 33141223 had an outstanding balance of $1,120.65 with the following account information:

Name: [redacted]
Registration Date: 8/7/2019

i. According to [redacted] records this [redacted] account, [redacted]@126.com, logged in from IP Address 36.97.143.26, the Yanbian Silverstar dedicated server, and received a total of $13,700.

ii. The [redacted] account had four additional email addresses in different names, consistent with the use of the [redacted] and email accounts by North Korean IT worker using multiple personas.

iii. One of the additional email addresses, [redacted]@gmail.com, was also used to register [redacted] account alongside the email address [redacted]@126.com, which includes the same "eden," a naming convention used by other DPRK IT workers and by [redacted]

z. [redacted] Cardholder ID: 32784117 had an outstanding balance of $35,684.77 with the following account information:

Name: [redacted]
Registration Date: 7/11/2019

i. [redacted] records revealed that the email address [redacted]@126.com registered a [redacted] account that was logged into from IP Address 1, indicating that the user has access to the Yanbian

Silverstar dedicated server, and that the user of this email address and related payment accounts is a Yanbian Silverstar North Korean IT worker.

ii. According to records from Microsoft, [redacted] wrote a [redacted] message on 10/18/19 that he sent $130 from the [redacted] after he discussed it with his "group leader." [redacted] records for the account with the email address [redacted]@126.com confirmed a $130 transaction on 10/18/19 with the note "Payment for the website updates". This confirms that the email address [redacted]@126.com and related payment accounts are controlled by [redacted]

iii. [redacted] records for the account with the email address [redacted]@126.com corroborated that the account is used for North Korean IT work, because the [redacted] account received $2,119,209.37 between 2019 to 2021, including money from the freelance worker platform [redacted]

[redacted] Connected Accounts

41. [redacted] fraud detection unit provided records for additional [redacted] accounts connected to the above accounts, and the FBI has corroborated that with its independent investigation. The following 5 accounts had an outstanding balance totaling $114,211.58:

42. A review of the accounts identified the following:

a. [redacted] Cardholder ID: 28235264 had an outstanding balance of $1,227.53 with the following account information:

Name: [redacted]

Registration Date: 9/13/2018

i. [redacted] records revealed that the [redacted] account registered with email address [redacted]@gmail.com was also registered with the email address [redacted]@gmail.com. Google records revealed that [redacted]@gmail.com has the recovery email address [redacted]@gmail.com. According to records from [redacted], the [redacted] account registered with the telephone number [redacted] (used by Individual 1 to contact [redacted] was registered using the email address [redacted]@gmail.com. This corroborates that the email account [redacted]@gmail.com is under the control of [redacted] a Yanbian Silverstar North Korean IT worker.

ii. A review of [redacted] records confirmed that this account received income from [redacted], a freelancer website. The account in turn sent over $164,000 to recipients in China, Pakistan, Russia, Panama, Hungary, Belarus, Ukraine, Cambodia, and the United States.

iii. A review of Microsoft records revealed a [redacted] from May 16, 2018 in which another North Korean IT worker requested that [redacted] send money to a [redacted] (freelance worker platform) via [redacted] using the email address [redacted]@comcast.net. The email address [redacted]@comcast.net is similar to [redacted]@gmail.com, corroborating that [redacted] controls this persona and related payment accounts.

b. [redacted] Cardholder ID 33534410 had a balance of $64,732.55 with the following account information:

Name: [redacted]
Registration Date: 9/5/2019

i. The [redacted] account of [redacted]@126.com shares a mailing address with the [redacted] account of [redacted]@126.com.

ii. According to [redacted] records from Microsoft, the [redacted] user [redacted] discussed IT work with [redacted] and twice sent the email address [redacted]@126.com to [redacted] user [redacted] to the [redacted] user [redacted] (the [redacted] username of Yanbian Silverstar Company President [redacted]), in Korean-language [redacted] about freelance IT work. Corroborating that [redacted]@126.com and related payment accounts is controlled by a North Korean IT worker, according to [redacted] records, the [redacted] account with the email address [redacted]@126.com logged into [redacted] from IP Address 1, indicating that the user has access to the Yanbian Silverstar dedicated server.

iii. Corroborating that [redacted]@126.com is a North Korean IT worker, the similar email address [redacted]@126.com was used to register a [redacted] account, also with the name [redacted] used to pay for the internet domain Silverstarchina.com, which is one of the websites used by Yanbian Silverstar to advertise their freelancer services.

iv. The [redacted] records show that during the period of February 2020 to November 2021, the account received $697,622.85 from [redacted]

accounts and sent $618,926.16 to [redacted] accounts in numerous countries, which again corroborates that this account is being used to launder North Korean IT worker payments.

c. [redacted] Cardholder ID: 38304950 had an outstanding balance of $14,222.00 with the following account information:

Name: [redacted]
Registration Date: 6/9/2020

i. Based on the number of payments from known North Korean IT workers and the amount, the FBI believes '[redacted] was recruited to open or use their [redacted] account to send/receive at their request and receive a percentage of the freelancer work completed by North Korean IT workers.

ii. [redacted] for [redacted]@gmail.com identified payments received from North Korean IT worker [redacted] account [redacted]@126.com. According to Microsoft [redacted] records, that email address was repeatedly sent, alongside a dollar amount, in text messages from [redacted] user [redacted] user [redacted] repeatedly discussed IT work with [redacted] including worker schedules, creating and logging into remote accounts, and purchasing virtual private servers).

iii. [redacted] records for [redacted]@126.com identified a payment of $100 to "[redacted]" using the email address [redacted]com on 11/29/2020. That same [redacted] account, [redacted]@126.com, paid $30 to an individual known to

provide false identification documents to North Korean IT workers, and received payments with notes indicating that the payment was for IT development work.

iv. The account received a total of $32,396 from a company called [redacted] which is a platform for hiring developers/freelancers. The account sent payments to individuals in India, Nigeria, and Pakistan totaling $19,896. Both of these payment patterns are consistent with North Korean IT workers money laundering behavior.

d. [redacted] Cardholder ID: 39675342 had an outstanding balance of $12,492.28 with the following account information:

Name: [redacted]
Registration Date: 8/29/2020

i. A review of Microsoft records of [redacted] conversations revealed that in 2020, [redacted] and another North Korean IT worker discussed payments for freelance IT work, and [redacted] discussed sending $551 to the [redacted] account using the email address [redacted]@126.com and received confirmation that the funds were received. North Korean IT workers use both [redacted] to facilitate the laundering of their proceeds. There is therefore probable cause to believe that the user of this email account and related payment accounts is a North Korean IT worker.

ii. A review of the bank accounts listed on the [redacted] account registered with the email address [redacted]@126.com identified 14 bank accounts all of which were listed in different names. The accounts were

located in Ukraine, Pakistan, United States, Sri Lanka, and Sweden. The use of multiple bank accounts in different names, all tied to one [redacted] account, corroborates that this account was utilized to launder North Korean IT worker payments.

e. [redacted] Cardholder ID: 46616965 had an outstanding balance of $21,537.22 with the following account information:

Name: [redacted]
Registration Date: 9/6/2021

i. A review of Microsoft records of [redacted] conversations between known Yanbian Silverstar North Korean IT workers, such as [redacted] user [redacted] discussing IT work in Korean message, revealed a message on 09/30/2021 in which [redacted]@126.com was discussed as the [redacted] account to be used to send money.

ii. The [redacted] account received two payments, one for $4,000 and the other for $490, from the [redacted] account of [redacted] Cardholder ID: [redacted]), whose email address, [redacted]@gmail.com, was used for the [redacted] account that sent funds to pay for the internet domain Silverstarchina.com, the public website used by Yanbian Silverstar to advertise their freelancer services.

iii. The [redacted] account sent two payments, one for $4,000 and the other for $490, from the [redacted] account of "[redacted]" ([redacted] Cardholder ID: [redacted]), whose email address, [redacted]@gmail.com, was used

for the [redacted] account that sent funds to pay for the internet domain Silverstarchina.com, the public website used by Yanbian Silverstar to advertise their freelancer services.

iv. According to [redacted] records, this account sent two $20,000 payments in April 2022 and May 2022 to the [redacted] account registered with the email address [redacted]@126.com, which had also received [redacted] payments in the amounts and dates requested on [redacted] by [redacted] user [redacted] (who has discussed IT work with [redacted] including worker schedules, account creation, interviewing for freelance IT work, and payments for freelance IT work), in [redacted] messages discussing Yanbian Silverstar North Korean IT work.

v. Corroborating that this account is used to launder North Korean IT worker funds, the [redacted] account sent, normally in $20,000 transactions, a total of $303,860.79, between October 2021 and January 2022.

[redacted] Similar Patterns of Activity Accounts

43. [redacted] provided records for an additional thirteen [redacted] accounts that show a similar pattern of activity as the above accounts, with a balance of $213,621.97. The FBI has independently corroborated that these accounts are linked to Yanbian Silverstar North Korean IT worker activity.

44. A review of the accounts identified the following:

a. [redacted] Cardholder ID: [redacted] had an outstanding balance of $20,001.90 with the following account information:

Name: [redacted]

[redacted]
Registration Date: 10/26/2021

i. In 2020, according to [redacted] records from Microsoft, [redacted] corresponded in Korean via [redacted] about IT projects with the [redacted] account registered with the email address [redacted]@gmail.com. According to records from Google, [redacted]@gmail.com accessed North Korea maps and a North Korean news site, the email account was used to apply for IT worker jobs, and the cloud storage contained resumes, job descriptions, interview scripts, and spreadsheets in Korean cataloging monthly revenue of various email addresses. The spreadsheet included payments to [redacted]@126.com of $2,500 on 1/10, and $6,000 on 1/20, and $2,400 on 1/26 (the year of the activity was not provided). There is therefore probable cause to believe that this email account and its associated payment accounts is used by a Yanbian Silverstar North Korean IT worker.

b. [redacted] Cardholder ID: 33024884 had an outstanding balance of $5,212.30 with the following account information:

Name: [redacted]
[redacted]
Registration Date: 7/30/2019
Registration IP address: 58.245.96.136 (China Unicom, Jilin, China)

i. The FBI observed the email address [redacted]@126.com being used on the website "[redacted].com," advertising web design services. This is

consistent with advertisements that North Koreans use for freelance IT work.

ii. A review of Microsoft records revealed a 1/15/20 [redacted] involving [redacted] (who discussed IT work with [redacted] including worker schedules, account creation, interviewing for freelance IT work, and payments for freelance IT work) in which [redacted] shared the name [redacted] and [redacted]

iii. A review of the [redacted] records for the account with the email account [redacted]@126.com identified a payment to an individual who had provided counterfeit U.S. driver's licenses, passports, and banking/bill statements to multiple North Korean IT workers to create and verify accounts on websites and platforms used for freelance work and payment.

iv. The account made withdrawals to a Chinese bank totaling $1,685,054.36 from 10/31/2019 to 4/19/2022, consistent with money laundering for North Korean IT workers.

c. [redacted] Cardholder ID: 33022701 had an outstanding balance of $27,962.19 with the following account information:

Name: [redacted]
Registration Date: 7/29/2019
Registration IP address: 58.245.96.136 (China Unicom, Jilin, China)

i. The above [redacted] account was created the day before the [redacted]@126.com [redacted] account, discussed previously in paragraph 44 subgraph b, from the same China-based IP address. Two

accounts created from the same IP address one day apart indicate they are both connected and therefore controlled by Yanbian Silverstar North Korean IT workers.

ii. A review of the [redacted] records for the account with the email account [redacted]@126.com identified a payment to an individual (the same individual paid by [redacted]@126.com) who had provided counterfeit U.S. driver's licenses, passports, and banking/bill statements to multiple North Korean IT workers to create and verify accounts on websites and platforms used for freelance work and payment.

d. [redacted] Cardholder ID: 35907047 had an outstanding balance of $18,514.78 with the following account information:

Name: [redacted]
Registration Date: 1/20/2020

i. A review of the [redacted] records for the account with the email account [redacted]@126.com identified a payment to an individual (the same individual paid by [redacted]@126.com and [redacted]@126.com) who had provided counterfeit U.S. driver's licenses, passports, and banking/bill statements to multiple North Korean IT workers to create and verify accounts on websites and platforms used for freelance work and payment.

ii. The account made withdrawals to a Chinese bank totaling $2,948,570.78 from 6/2/2020 to 4/23/2022 and received $2,873,306.71 from other

[redacted] accounts, consistent with money laundering by North Korean IT workers.

e. [redacted] Cardholder ID: 37861277 had an outstanding balance of $11,383.57 with the following account information:

Name: [redacted]
Registration Date: 5/18/2020

i. A review of the [redacted] records for the account with the email account [redacted]@126.com identified a payment to an individual (the same individual paid by [redacted]@126.com, [redacted]@126.com, and [redacted]@126.com) who had provided counterfeit U.S. driver's licenses, passports, and banking/bill statements to multiple North Korean IT workers to create and verify accounts on websites and platforms used for freelance work and payment.

ii. This [redacted] account also received $20,003 from the [redacted] account [redacted] Cardholder ID: 33022701, with email address [redacted]@126.com, listed above.

iii. This [redacted] account received $2,672,259.29 from various [redacted] accounts, $562,500 from the [redacted] account registered with the same email address, sent $3,092,503 to a Chinese bank, and sent $129,704.50 to other [redacted] accounts, all of which is consistent with money laundering activity by North Korean IT workers.

f. [redacted] Cardholder ID: 39420481 had an outstanding balance of $45,533.12 with the following account information:

Name: [redacted]
Registration Date: 8/12/2020

i. The [redacted] records show that during the period of May 2021 to April 2022, the account received $386,450.00 from other [redacted] accounts, sent $70,685.00 to other [redacted] accounts, and withdrew a total of $299,750.00 to a bank account in China. This is consistent with money laundering activity by North Korean IT workers.

ii. The address provided by the user is Dandong, is a city in China on the border of North Korea, which is a location used by Yanbian Silverstar North Korean IT workers.

iii. Corroborating that this user is a North Korean IT worker, they provided information to [redacted] that they do web programming, and provided job platform [redacted] as their business website.

g. [redacted] Cardholder ID: 35779452 had an outstanding balance of $3,000 with the following account information:

Name: [redacted]
Registration Date: 1/11/2020

i. The account was looked up from IP address 188.43.136.32,[1] which resolves to TransTeleCom (TTK), Russia, on 8/17/2020.

[1] The IP address range 188.43.136.0–188.43.136.255, which can be written as 188.43.136.0/24, are controlled, and used by North Korea. The IP address range has the network name of KPOST, which the name of North Korea's government agency responsible for their telecommunications.

ii. The FBI's investigation observed that other Yanbian Silverstar North Korean IT workers logged into their payment platform accounts from the IP address 188.43.136.32 and others in 188.43.136.0/24. Additionally, a private sector freelancer platform who is frequently used by North Korean IT workers, reported to the FBI that North Koreans have created accounts using IP addresses from the 188.43.136.0/24 range.

iii. The [redacted] account uses '[redacted]' as an answer to a security question. The FBI has observed North Koreans use "PY" to represent Pyongyang, the capital of North Korea.

iv. This [redacted] user linked their account to their profile on [redacted], a freelancer platform which is frequently used by North Korean IT workers, which indicates that they are located in Yanji, the main location for the Yanbian Silverstar group.

h. [redacted] Cardholder ID: 48158330 had an outstanding balance of $13,067.59 with the following account information:

Name: [redacted]

Registration Date: 11/22/2021

i. According to [redacted] records from Microsoft, in 2021, the [redacted] user [redacted] (who has discussed IT work with [redacted] including worker schedules, account creation, interviewing for freelance

Additionally, TTK released a statement that stated they provide services for North Korea through Korea Posts and Telecommunications (KPOST).

IT work, and payments for freelance IT work) frequently sent the email address [redacted]@126.com along with dollar amounts. [redacted] records revealed that these dates and dollar amounts corresponded to payments received by this account. Based on these [redacted] and their context, there is probable cause to believe the email address [redacted]@126.com is controlled and used by the user of [redacted] for Yanbian Silverstar North Korean IT work.

ii. According to [redacted] records, this account received two $20,000 payments in April 2022 and May 2022 from [redacted] account [redacted] Cardholder ID: 46616965), who was previously discussed as a recipient of Yanbian Silverstar North Korean IT worker proceeds.

i. [redacted] Cardholder ID: 46165387 had an outstanding balance of $216.83 with the following account information:

Name: [redacted]
Registration Date: 8/14/2021

i. According to Slack records, the channel [redacted] slack.com, which Yanbian Silverstar North Korean IT workers used to catalog numerous entries described as "weekly payments for app development," the email address [redacted]@126.com along with a reference to [redacted] and dollar amounts appear in multiple direct messages in Korean in 2021. This is probable cause to believe that the user of this account is a North Korean IT worker.

j. [redacted] Cardholder ID: 48112708 had an outstanding balance of $7,038.10 with the following account information:

Name [redacted]
Registration Date: 11/20/2021

i. According to [redacted] records, [redacted] account was created using the same computer[2] as the [redacted] account of [redacted] (an account discussed in paragraph 44, subparagraph h), Cardholder ID 48158330 (Target Account). [redacted] records include a hash or unique fingerprint of the computer used to create the account. [redacted] accounts shared the same unique identifier. [redacted] had received [redacted] payments in the amounts and dates requested on [redacted] by [redacted] user [redacted] who had discussed IT work with [redacted] including worker schedules, account creation, interviewing for freelance IT work, and payments for freelance IT work). [redacted] account was created on 11/20/2021. [redacted] account was created on 11/22/2021. The creation of two different accounts from the same computer in the same week shows the same Yanbian Silverstar North Korean IT worker controlled both accounts.

k. [redacted] Cardholder ID: 29427034 had an outstanding balance of $16,946.33 with the following account information:

Name: [redacted]

2 [redacted] This cardholder account (48112708) and 48158330 had the same fingerprint (unique identifier).

[redacted]
Registration Date: 02/02/2018

i. According to [redacted] records, this account sent multiple payments to [redacted] (Ukraine, [redacted] Cardholder ID 18398037) in 2020. After these payments, [redacted] made payments to [redacted] ID 33534410, [redacted], who is described above as a North Korean IT worker who laundered money for Yanbian Silverstar IT workers and made payments for the Yanbian Silverstar internet domain.

ii. According to [redacted] records, this account sent payments to [redacted] (Ukraine, [redacted] Cardholder ID 33128384) in 2019. This [redacted] account received payments in 2019 from [redacted] account [redacted] ([redacted] Cardholder ID 28739311), who is described above as a North Korean IT worker who made payments for the Yanbian Silverstar internet domain.

iii. The [redacted] records show that this account received $2,410,796.16 from other [redacted] accounts, which corroborates that it is used for North Korean IT Worker money laundering activity.

l. [redacted] Cardholder ID: 48129187 had an outstanding balance of $11,774.00 with the following account information:

Name: [redacted]
Registration Date: 11/21/2021

i. According to [redacted] records, this account received a total of $38,750, in 16 payments, from December 2021 to April 2022, from [redacted] account [redacted] Cardholder ID: 40923961), whose user sent funds to pay for the Yanbian Silverstar internet domain.

i. According to [redacted] records, this account received a total of $60,500, in four payments, three of which were $20,000 from January to February 2022, from [redacted] account [redacted] Cardholder ID: 46616965), who is described above as sending and receiving Yanbian Silverstar North Korean IT worker proceeds.

m. [redacted] Cardholder ID: 48391426 had an outstanding balance of $32,971.26 with the following account information:

Name: [redacted]
Registration Date: 12/03/2021

i. According to [redacted] records [redacted] received a total of $414,030.56 from December 2021 to April 2022.

ii. This account received money in 2022 from "[redacted]" [redacted] Cardholder ID 32106457, Odessa, Ukraine, who in turn received multiple payments from [redacted] Cardholder ID 29427034, which is described above as an account sending and receiving Yanbian Silverstar North Korean IT worker proceeds.

SEIZURE PROCEDURE FOR TARGET ACCOUNTS

45. 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 money laundering violations.

46. Should this seizure warrant be granted, law enforcement intends to work with [redacted] seize the funds contained within the **Target Accounts** by transferring the funds to a U.S. government-controlled account at [redacted]

47. 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

48. 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.

49. 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.

[redacted]
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 [redacted] day of October, 2022.

[redacted]
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 (the "**Target Accounts**") by serving this warrant on [redacted]

	Cardholder ID	Email	Registration Date	Amount
1	32787138	[redacted]	7/12/2019	$230,451.28
2	32823195	[redacted]	7/15/2019	$79,400.84
3	26364278	[redacted]	4/27/2018	$75,054.35
4	27361057	[redacted]	7/12/2018	$73,258.78
5	27738625	[redacted]	7/12/2018	$45,934.74
6	41482927	[redacted]om	12/14/2020	$36,413.40
7	33072116	[redacted]	8/2/2019	$33,190.57
8	27851354	[redacted]	8/15/2018	$27,810.94
9	43552963	[redacted]	4/20/2021	$25,134.92
10	41509922	[redacted]	12/15/2020	$24,976.32
11	43476624	[redacted]	4/16/2021	$22,972.28
12	33012110	[redacted]com	7/29/2019	$19,128.39
13	32820879	[redacted]	7/14/2019	$18,776.61
14	28661935	[redacted]	10/14/2018	$14,111.60
15	32775158	[redacted]	7/11/2019	$9,361.25
16	32006723	[redacted]	5/13/2019	$7,245.00
17	40923961	[redacted]	11/9/2020	$6,115.55
18	33056635	[redacted]	8/1/2019	$6,071.58
19	32016016	[redacted]	5/14/2019	$3,743.36
20	33145450	[redacted]	8/7/2019	$3,368.60
21	33352633	[redacted]m	8/23/2019	$2,711.49
22	45177501	[redacted]	7/1/2021	$1,739.80
23	28739311	[redacted]	10/19/2018	$1,447.26
24	42779276	[redacted]	3/4/2021	$1,292.79
25	33141223	[redacted]	8/7/2019	$1,120.65
26	32784117	[redacted]m	7/11/2019	$35,684.77
27	28235264	[redacted]m	9/13/2018	$1,227.53
28	33534410	[redacted]	9/5/2019	$64,732.55
29	38304950	[redacted].com	6/9/2020	$14,222.00
30	39675342	[redacted]	8/29/2020	$12,492.28
31	46616965	[redacted]	9/6/2021	$21,537.22

32	47599874	[redacted]	10/26/2021	$20,001.90
33	33024884		7/30/2019	$5,212.30
34	33022701		7/29/2019	$27,962.19
35	35907047		1/20/2020	$18,514.78
36	37861277		5/18/2020	$11,383.57
37	39420481		8/12/2020	$45,533.12
38	35779452		1/11/2020	$3,000.00
39	48158330		11/22/2021	$13,067.59
40	46165387		8/14/2021	$216.83
41	48112708		11/20/2021	$7,038.10
42	29427034		2/2/2018	$16,946.33
43	48129187		11/21/2021	$11,774.00
44	48391426		12/3/2021	$32,971.26
			TOTAL	**$1,134,350.67**