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. 4:24MJ9029 RHH

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

January 11, 2024 at 3:43 p.m.
Date and Time Issued

at St. Louis, Missouri
City and State [redacted]

Honorable Rodney H. Holmes, U.S. Magistrate Judge
Name and Title of Judicial Officer

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 $312,642.55 USD and $10,358.52 CAD held in the specific 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") 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, Jong Song Hwa, 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 opened an investigation into Yanbian Silverstar after the identification of an individual who allowed another individual, subsequently identified as a North Korean IT worker, to use their online freelancer account at a U.S. based freelancer platform. Additionally, the individual allowed the North Korean IT worker to remotely access a laptop on their network for freelance work and was paid $100 per month per laptop for it. The investigation identified financial accounts associated to Yanbian Silverstar and other North Korean IT worker groups.

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

24. In order to further disrupt North Korean IT workers, the FBI conducts outreach and notifications to companies who have inadvertently hired a North Korean IT worker, including IT staffing firms. The notification process includes a threat awareness briefing about the North Korean IT worker threat and the methodologies and tactics used by North Korean IT

workers to obtain employment. Additionally, the FBI provides indicators companies can use to identify suspicious remote workers, including U.S. Government publically available advisories,

25. On or about September 25, 2023, I provided a North Korean IT worker threat awareness brief to an IT staffing firm's executive manager and their head of Human Resources (HR) operations, herein referred to as U.S. IT Staffing Firm 1. The U.S. IT Staffing Firm 1 was provided indicators to look for suspicious remote workers. For example, the FBI provided the following indicators:

a. Use of emails addresses in names different than who they purport to be;

b. Changing their home address upon hiring or receiving a company device;

c. Multiple changes to their bank account information;

d. Unfamiliarity with their location;

e. Not able to travel or meet in person;

f. Unable to use web camera;

g. Having outside assistance with technical or job interviews;

h. Unable to comply with short notice requests for information or documentation;

i. Inability to verify education, references, or other application information; and

j. Use of certain banks for payment.

26. On or about October 16, 2023, using the information received in the North Korean IT worker threat brief, I received a list of 10 suspicious remote workers who had been previously hired by IT Staffing Firm 1 and contracted to work at various U.S. based employers in IT related fields. IT Staffing Firm 1 provided the remoter worker's name, email address, address, employer, and bank account information.

27. A review of the information identified two of the ten remote workers had used a

name or an email address the FBI previously observed in its investigation being used by North Korean IT workers. For example, one of the names and address was of an individual who had been previously employed at a company headquartered in the Eastern District of Missouri referred to as U.S. Business 1, who had notified the FBI of the suspicious remote workers, based on the publically available advisory. Subsequent investigation into the identity, determined the name of the individual was assisting North Korean IT workers by receiving laptops from employers who inadvertently hired North Korean IT workers.

28. A review of the bank account information provided by IT Staffing Firm 1 identified financial institutions known to your affiant to be used by Payment Service Provider 1 to provide "virtual account numbers", which is a service allowing the account holder to receive a U.S. bank account number and receive deposits into their Payment Service Provider 1 account. This allows individuals, including those who are not U.S. citizens or reside in the U.S., to receive payment in USD, which can be exchanged into the currency of their choice. North Korean IT workers exploit the virtual account number service by opening an account using an identity, typically a Chinese national, at the Payment Service Provider 1 and obtaining a U.S. bank account number. The U.S. bank account information is provided to the U.S. based employer who is unaware the payments are ultimately being made to an account in the name of a different person and typically a foreign national. Once money is in the account, it can be transferred to Chinese banks and converted to CNY (Chinese Yuan). North Korean IT workers share the virtual account numbers amongst their team members and associates so multiple workers can receive payments to the same Payment Service Provider 1 account in different names. This technique allows North Korean IT workers to mask their true identity and location and appear to be located in the United States. It further allows the revenue generated to be controlled by

certain individuals and lessen the need to manage multiple payment accounts.

29. Payment Service Provider 1 can provide subscriber records based on the virtual account number. On or about November 23, 2023, Payment Service Provider 1 provided records for the virtual account numbers received from IT Staffing Firm 1. A review of the records identified information indicative of North Korean IT workers receiving payments for freelancer work, as well as money laundering. For example, some accounts had bank accounts associated with online banks, banks which allow users to create an account online, in in different names. This means North Korean IT workers can create accounts online using identifiers they obtain. Also, accounts received multiple payments from various freelancer companies and staffing firms in different names and there were recurring withdrawals to Chinese bank accounts of $10,000 USD and $20,000 USD. Several of the accounts had submitted suspected fraudulent identity documents and the accounts had logins from various Virtual Private Network (VPN) IP addresses, which mask their true location.

30. The FBI conducted additional analysis of the Payment Service Provider 1 accounts identified, and a subset of those accounts are the funds in the **Target Accounts** to be seized in Attachment A.

31. The **Target Accounts**, which comprise of three Payment Service Provider 1 accounts holding $312,642.55 USD in two accounts and $10,358.52 CAD[1] in one account in proceeds from the fraud scheme, are further described below. The subscriber information listed below for each account was provided by Payment Service Provider 1.

1 The account's balance is stored at Payment Service Provider 1 in CAD and will be converted to USD by Payment Service Provider 1 prior to sending it to the FBI at the current exchange rate. Due to changing of currency exchange rates, the FBI lists the balance as CAD to accurately reflect the current amount of funds remaining in the account.

a. Payment Service Provider 1 Account Holder ID: 57076178 has an outstanding balance of $286,808.48 USD with the following account information:

Name: [redacted]
Address: [redacted]
Email: [redacted]
Registration Date: 08/18/2022

i. During the period of October 2022 to June 2023, the 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, almost weekly. This money movement and withdrawals are consistent with an account used by North Korean IT workers to launder money.

ii. The account received payments from a virtual account number from various companies in 23 different names. One of these companies was U.S. IT Staffing Firm 1 who sent the payment for "K.S." (redacted). The email address provided to U.S. IT Staffing Firm 1 was [redacted] and listed an address in Houston, Texas. The use of a different name for an email address ([redacted], not K.S.) and the use of the word "dev", short for developer, is frequently seen in email addresses used by North Korean IT workers.

iii. Payment Service Provider 1 requires the account holders to answer questions in order to receive payments. The account holder stated they use the account to receive payments from marketplaces they sell on, such as Amazon, Etsy, Wayfair, Google, and Apple and for payments from

business they work with such as clients, employers, or other business partners. No payments were received from the online marketplaces they listed. Additionally, they stated they provide "web programming services" and provided a URL to a U.S. based freelancer marketplace. On or about November 29, 2023, a review of the freelancer profile listed indicated the user had been working on the platform since December 2011, and had been hired once for a total of $235, an amount not close the over $700,000 received at the account. It is a common technique for North Korean IT workers to create profiles at freelancer platforms to get jobs and to use them to get financial accounts approved.

iv. A review of the account registration information identified a security answer of "kcc". Security answers are provided in case a user forgets their password and needs it be reset. The use of "kcc" is believed to be a reference to the Korea Computer Center (KCC) which was a North Korean information technology research center within the 313 General Bureau, North Korea's department which deploys a majority of North Korea's IT work force. North Korean IT workers frequently use words or dates associated with North Korea.

v. A review of the documents provided by the customer to verify their account identified multiple generic invoices for purported IT work which only listed the name of the developer, along with [redacted], and a company name. These invoices were identical in the layout to the ones observed in the **Target Account**, Account Holder ID: 46923548, discussed later, and

are believed to be created for the purpose of account verification at Payment Service Provider 1. Additionally, a "Software Development Contract" purportedly created by a company and signed by [redacted] listed the incorrect CEO for the company, indicating the software contract was fraudulently created.

vi. A review of the IP login for the account identified the user primarily logged in from IP addresses which resolved to South Korea and only once from Dandong, China, the purported location of the account holder. North Korean IT workers frequently utilize VPNs or proxy services to mask their true location and attempt to use the same IP address location when accessing the account in an attempt to avoid the account being flagged for suspicious or fraudulent activity.

b. Payment Service Provider 1 Account Holder ID: 28466333 has an outstanding balance of $25,834.07 USD with the following account information:

Name: [redacted]
Address: [redacted]
Email: [redacted]
Registration Date: 09/30/2018

i. During the period of October 2018 to February 2023, the account received $4,342,403.51 USD from [redacted], an online marketplace to sell digital items, such as website templates. From October 2019 to March 2023, the account received $423,174.56 for suspected freelancer work and from another Payment Service Provider, identified as Payment Service Provider 2. From October 2019 to December 2019, the account withdrew

a total of $197,467.94 USD to bank accounts at [redacted], [redacted], and [redacted] with several amounts over $20,000 with the largest of $60,000. From January 2019 to March 2023, the account sent $4,588,534.70 to other Payment Service Provider 1 accounts and received $120,531.10. This money movement and withdrawals are consistent with an account used by North Korean IT workers to launder money.

ii. Payment Service Provider 1 requires the account holders to answer questions in order to receive payments. The account holder stated they use the account to receive payments from selling web framework themes on Envato marketplace and they provided a link to their online profile with the user name "[redacted]". A review of [redacted] for "[redacted]" identified a website at [redacted] and an email address [redacted]. A review of records obtained from a search warrant at Microsoft for North Korean IT worker accounts, identified emails to an identified North Korean IT worker, working on behalf of Yanbian Silverstar, from "Alex", [redacted], whose automatic email reply listed the email address [redacted]. Another email to the identified North Korean from [redacted], dated November 26, 2019, was in Korean and requested him to be contacted. The email was signed as [redacted], which translated from Korean to English is "[redacted]", with the last name unknown (LNU). An online chat communication from the

Microsoft search warrant identified a conversation on December 2, 2019, between the identified North Korean and the user, [redacted]. The user subsequently replied on December 27, 2019, and they discussed issues at the online freelancer platform and their training and travel plans. The FBI believes, Alex, also known as LNU [redacted], a suspected North Korean IT worker, works as "[redacted]" on [redacted] selling web framework themes, and used the persona "[redacted]" to receive payments.

iii. On January 30, 2023, the account received a payment from U.S. IT Staffing Firm 1 to their virtual account number in the name "E.D." (redacted). The email address provided to U.S. IT Staffing Firm 1 was [redacted] and an address in Miami, FL. The bank account information for the contractor at the U.S. IT Staffing Firm 1 was changed 6 times from January 9, 2023 to June 23, 2023. Five of these accounts corresponded to other Payment Service Provider 1 accounts in different names, other than E.D., and in different locations in the United States and China. One of those additional bank accounts corresponds to one of the **Target Accounts**, Account Holder ID: 46923548, discussed in the next section. The changing of bank accounts and the reuse of bank accounts across different identifies at an IT staffing firm is a common technique used by North Korean IT workers.

iv. A review of the documents provided by the account holder to verify their communication with their freelance customers, identified a software

contract with a U.S. business in the name of "[redacted]" with an address in California, and an invoice to the same company using the name "[redacted]" with an address in Miami, FL, the same one provided by E.D. The use of "[redacted]" in documents provided to Payment Service Provider 1, but a different name than used with U.S. IT Staffing Firm 1, is a technique used by North Korean IT workers to get their financial accounts approved.

v. A review of the IP login for the account identified the user primarily logged in from IP addresses which resolved to United States from providers who typically provide VPN or proxy services. North Korean IT workers frequently utilize VPNs or proxy services to mask their true location.

c. Payment Service Provider 1 Account Holder ID: 46923548 has an outstanding balance of $10,358.52 CAD with the following account information:

Name: [redacted]
Address: [redacted]
Email [redacted]
Registration Date: 09/23/2021

i. During the period of October 2021 to June 2023, the account received $1,457,809.57 USD for suspected freelancer work in the names of 13 different people and from various companies. From November 2021 to May 2023, the account received $266,276.42 CAD for suspected freelancer work in the names of 4 different people and a company. From October 2021 to June 2023, the account had 73 withdrawals totaling

$1,799,670.00 USD to a bank account at [redacted] with the average withdrawal amount of close to $25,000. From November 2021 to February 2022, the account had 4 withdrawals totaling $98,585.00 CAD to the same bank in China. From January 2022 to June 2023, the account sent $116,029.59 to other Payment Service Provider 1 accounts in China and received $306,841.70 from accounts in various countries such as China, Turkey, Pakistan, Bangladesh, Vietnam, and others. This money movement between accounts and withdrawals are consistent with an account used by North Korean IT workers to launder money.

ii. From January 3, 2023 to June 7, 2023, the account received payments totaling $90,096.20 from U.S. IT Staffing Firm 1 to their virtual account number for freelance work in the name of "C.H." (redacted). The email address provided to U.S. IT Staffing Firm 1 was "c.h." [redacted] (redacted) and an address in Springdale, AR. The bank account information for the contractor at U.S. IT Staffing Firm 1 was changed 4 times from December 19, 2022 to June 19, 2023. One of these bank accounts corresponds to the **Target Account**, Account Holder ID: 28466333, discussed previously. The changing of bank accounts and the reuse/sharing of bank accounts across different identities at an IT staffing firm is a common technique used by North Korean IT workers.

iii. A review of the documents provided by the customer to verify their identity revealed they used a Chinese national identification card of an Asian female. However, the name used to receive payment from U.S. IT

Staffing Firm 1 used the name "C.S." who purported to be male. North Korean IT workers almost exclusively apply for freelance work as a male, since they themselves are male, but they do not have a preference for their financial accounts. They will recruit individuals, typically Chinese nationals, to use their identifiers and identity documents to open a financial account. However, the North Korean IT worker creates and maintains access to the financial account, not the recruited individual.

iv. A review of the documents provided by the account holder to verify their account identified multiple generic invoices for purported IT work which listed the name of the developer, "[redacted]", and different company names. These invoices were identical in the layout to the ones observed in the **Target Account**, Account Holder ID: 57076178, discussed previously, and are believed to be created for the purpose of account verification at Payment Service Provider 1.

v. Payment Service Provider 1 requires the account holders to answer questions in order to receive payments. The account holder related they provide mobile apps and operate the website "[redacted]" as a software engineer. On December 6, 2023, open source research was conducted for [redacted] and the domain no longer resolved. It was registered on September 27, 2021, four days after the "[redacted]" account was registered at Payment Service Provider 1. A review of the Internet Archive's Wayback Machine identified a capture of [redacted] from December 16, 2021, which had a website for the company "[redacted]", a software

development company in Toronto, Ontario, Canada. It contained a list of developers which did not include "[redacted]". The use of websites and software development companies, is a common tactic by North Korean IT workers to make it appear as they are located in a different country and further obfuscates their North Korean identity.

SEIZURE PROCEDURE FOR TARGET ACCOUNTS

32. 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.

33. 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.

34. 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

35. 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.

36. 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 11th day of January, 2024.

[redacted]
HONORABLE RODNEY H. HOLMES
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]:

	Account Holder ID	Email	Registration Date	Amount
1	57076178	[redacted]	08/18/2022	$286,808.48
2	28466333	[redacted]	09/30/2018	$25,834.07
			Total USD	**$312,642.55**
3	46923548	[redacted]	09/23/2021	$10,358.52
			Total CAD	**$10,358.52**