IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Holding a Criminal Term
Grand Jury Sworn in on April 11, 2024

UNITED STATES OF AMERICA	:	**CRIMINAL NO.**
	:	
v.	:	**VIOLATIONS:**
	:	
CHRISTINA CHAPMAN,	:	**18 U.S.C. § 371 (Conspiracy to Defraud the United States)**
JOHN DOE 1, alias JIHO HAN,	:	
	:	**18 U.S.C. §§ 1343, 1349 (Conspiracy to Commit Wire Fraud)**
JOHN DOE 2, alias HAORAN XU,	:	
	:	**18 U.S.C. §§ 1344, 1349 (Conspiracy to Commit Bank Fraud)**
JOHN DOE 3, alias CHUNJI JIN,	:	
	:	**18 U.S.C. § 1028A(a)(1) (Aggravated Identity Theft)**
Defendants.	:	
	:	**18 U.S.C. §§ 1028(a)(7), (b)(1)(D), (c)(3)(A) & (f) (Conspiracy to Commit Fraud and Related Activity in Connection with Identification Documents)**
	:	
	:	**18 U.S.C. §§ 1956(a)(1)(B)(i) & (h) (Conspiracy to Launder Monetary Instruments)**
	:	
	:	**18 U.S.C. § 1960 (Prohibition of Unlicensed Money Transmitting Business)**
	:	
	:	**8 U.S.C. § 1324a (Unlawful Employment of Aliens)**
	:	
	:	**18 U.S.C. § 2 (Aiding and Abetting)**
	:	

INDICTMENT

The Grand Jury charges that, at times material to this Indictment:

COUNT ONE
(Conspiracy to Defraud the United States)

INTRODUCTION

1. Since 2003, the Democratic People's Republic of Korea ("DPRK" or "North Korea") has been under sanction by the United Nations ("UN") due to its testing and expansion of its nuclear weapons program. Since 2016, the United States has had comprehensive sanctions against North Korea, cutting it off from the U.S. financial system and limiting the ability of U.S. persons and companies to do business with North Koreans. As a result, North Korea has sponsored various subterfuge schemes to earn money for the regime.

2. According to a May 2022 advisory by the Department of State, the Department of the Treasury, and the Federal Bureau of Investigation, North Korea has dispatched thousands of highly-skilled information technology ("IT") workers around the world, earning revenue that contributes to the North Korean weapons programs, in violation of U.S. and UN sanctions. These workers (i) misrepresent themselves as foreign (non-North Korean) or U.S.-based teleworkers, including by using virtual private networks ("VPNs"), virtual private servers ("VPSs"), third-country internet protocol ("IP") addresses, proxy accounts, and falsified or stolen identification documents; (ii) surreptitiously obtain IT development employment from companies spanning a range of sectors and industries around the world; (iii) develop applications and software for their employers; and (iv) in some instances, use privileged access gained through such employment for illicit purposes, including enabling malicious cyber intrusions by other DPRK actors into an employer's network. These IT workers are often subordinate to North Korea's Munitions Industry Department ("MID"). MID is involved in key aspects of North Korea's weapons program, including overseeing the development of North Korea's ballistic missiles, weapons production, and research and development programs.

3. From in or around early 2020 until the present, one group of overseas IT workers has been perpetrating such a coordinated scheme to conduct remote work for U.S. companies, resulting in the transmission of false information to the United States and its agencies. Specifically, this group of overseas IT workers has stolen the identities of U.S. nationals; applied for remote jobs in the United States through the transmission of false documentation to the Department of Homeland Security ("DHS"); obtained jobs at hundreds of U.S. companies, to include Fortune 500 companies, often indirectly through staffing companies or other contracting organizations ("staffing companies"); received laptop computers and other hardware from U.S. companies through which they have access to the internal systems of the U.S. companies (generally, "laptops"); and been paid millions of dollars for their work, much of which has been falsely reported to the Internal Revenue Service ("IRS") and the Social Security Administration ("SSA") in the name of the actual U.S. persons whose identities have been false, stolen, or borrowed. The overseas IT workers have been assisted in this scheme by various U.S. nationals, who have acted knowing that the overseas IT workers were, in fact, not located in the United States, that they used false, stolen, or borrowed identities belonging to real U.S. persons, and that they were defrauding the U.S. companies.

4. From in or around October 2020, until on or about October 26, 2023, Christina Marie CHAPMAN, a U.S. national, conspired with certain overseas IT workers to affect a scheme to defraud the United States and its agencies. Specifically, CHAPMAN: (i) assisted the overseas IT workers in validating stolen identity information of U.S. citizens so the overseas IT workers could pose as U.S. citizens; (ii) received and hosted laptops issued by U.S. companies to the overseas IT workers in her U.S. residences (a "laptop farm"), so that the companies believed the workers to be located in the United States, and sent other laptops from her residences to overseas

IT workers abroad; (iii) at her laptop farms, logged into the U.S. companies' laptops and assisted the overseas IT workers with connecting remotely, so it appeared that the logins were coming from the United States; and (iv) received paychecks for the overseas IT workers at her home, forged the signatures of the beneficiary on the checks, and deposited them to her U.S. financial institution, thereafter further transferring the proceeds of the scheme to the overseas IT workers. In exchange, CHAPMAN charged monthly fees to the overseas IT workers for her services, enriching herself off the scheme.

5. The conspiracy perpetrated a staggering fraud on a multitude of industries, at the expense of generally unknowing U.S. companies and persons. It impacted more than 300 U.S. companies, compromised more than 60 identities of U.S. persons, caused false information to be conveyed to DHS on more than 100 occasions, created false tax liabilities for more than 35 U.S. persons, and resulted in at least $6.8 million of revenue to be generated for the overseas IT workers. The overseas IT workers worked at blue-chip U.S. companies, including a top-5 national television network and media company, a premier Silicon Valley technology company, an aerospace and defense manufacturer, an iconic American car manufacturer, a high-end retail chain, and one of the most recognizable media and entertainment companies in the world, all of which were Fortune 500 companies. The overseas IT workers also exfiltrated data from at least two U.S. companies—a multinational restaurant chain and a classic American clothing brand. The overseas IT workers also attempted to gain employment and access to information at two different U.S. government agencies on three different occasions, although these attempts were discovered and thwarted, due to the agencies' enhanced due diligence.

BACKGROUND

A. Sanctions Against North Korea

6. In December 1985, North Korea ratified the Nuclear Non-Proliferation Treaty ("NPT"). On January 10, 2003, North Korea withdrew from the NPT. On October 14, 2006, the UN Security Council passed Resolution 1718 condemning North Korea's first nuclear test and imposed sanctions on North Korea, including the supply of heavy weapons and select luxury goods. After successive nuclear tests by North Korea, the UN Security Council strengthened or imposed additional sanctions in 2009, 2013, 2016, and 2017.

7. The International Emergency Economic Powers Act ("IEEPA"), codified at Title 50 U.S.C. § 1701 *et seq.*, enacted in 1977, authorizes the President to impose economic sanctions in response to an unusual or extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security, foreign policy, or economy of the United States when the President declares a national emergency with respect to that threat. Pursuant to that authority, on March 15, 2016, the President issued EO 13722 addressing the Government of North Korea's continuing pursuit of its nuclear and missile programs. EO 13722 imposed a comprehensive blocking of the Government of North Korea and the Workers' Party of Korea. Pursuant to that authority, on March 16, 2016, the Secretary of the Treasury promulgated the "North Korea Sanctions Regulations." *See* 31 C.F.R. § 510.101 *et seq.* (amended 83 Fed. Reg. 9182 (Mar. 5, 2018)). These authorities generally prohibited the exportation and re-exportation of goods, services (including financial services), and technology to North Korea, unless exempt or authorized by the Department of the Treasury. Under these orders, U.S. financial institutions were barred from providing banking services to North Korea entities. These authorities barred any

transaction by any U.S. person or within the United States that evaded or avoided, or had the purpose of evading or avoiding, any prohibition set forth in these Executive Orders or regulations.

8. The Bank Secrecy Act requires U.S. financial institutions to take anti-money laundering measures to ensure that U.S. bank accounts are not used to finance terrorism or to avoid sanctions programs administered by the Department of the Treasury. The Treasury Department's Financial Crimes Enforcement Network ("FinCEN") is responsible for administering the Bank Secrecy Act in furtherance of its mission to safeguard the U.S. financial system. FinCEN is located in Washington, D.C. The Bank Secrecy Act gives FinCEN a range of options, called special measures, which can be adapted to target specific money laundering and terrorist financing concerns. *See* USA PATRIOT Act § 311, codified at 31 U.S.C. § 5318A. Under this authority, in June 2016, FinCEN determined that the entire North Korean financial sector was a "primary money laundering concern." Federal Register, Vol. 81, No. 107 (June 3, 2016). On November 9, 2016, FinCEN implemented a special measure, effectively barring all North Korean financial institutions and entities acting on their behalf from engaging in U.S. dollar transactions in the United States. Failure to comply with the special measure resulted in civil and criminal penalties for U.S. financial institutions. As a result of the North Korea sanctions, the FinCEN 311 action, and overall risk management, beginning in at least March 2016, U.S. banks refused to knowingly process any U.S. dollar wire transactions involving entities in North Korea.

B. U.S. Work Authorization and the Relevant Federal Agencies

9. DHS U.S. Citizenship and Immigration Services ("USCIS") is the federal agency responsible for ensuring employment eligibility for workers in the United States. DHS and USCIS are located in the District of Columbia.

a. Federal law requires that every U.S. employer who recruits, refers for a fee, or hires an individual for employment in the United States must complete Form I-9, Employment Eligibility Verification ("Form I-9"). A Form I-9 must be completed for every individual hired for employment in the United States, including citizens and noncitizens. On the form, an employee must attest to their employment authorization. The employee must also present their employer with acceptable documents as evidence of identity and employment authorization. The employer must examine these documents to determine whether they reasonably appear to be genuine and relate to the employee, then record the document information on the employee's Form I-9. Employers must have a completed Form I-9, on file for each person on their payroll (or otherwise receiving remuneration) who is required to complete the form.

b. As a voluntary alternative to the Form I-9 process, employers may use E-Verify, a web-based system run by USCIS. In the E-Verify process, employers create cases based on information taken from an employee's Form I-9. E-Verify then electronically compares that information to records available to DHS and SSA. E-Verify generates a response to the employer confirming the employee's employment eligibility or indicating that the employee needs to take further action to complete the case. Although E-Verify requires the use of a photographic identity document, it does not have the ability to query submitted state drivers' license photographs against the state drivers' license databases.

c. Prior to August 2023, U.S. employers were generally required to review employment eligibility documents in person. After August 2023, employers could

remotely examine and submit employment eligibility documentation through E-Verify.

10. IRS is the federal agency responsible for collection of taxes from U.S. employers and employees. IRS is located in the District of Columbia. Generally, U.S. employers withhold federal taxes from the pay checks of their employees and transmit those funds to the United States government. Generally, U.S. employers transmit to IRS reports of the total wages earned and the total taxes withheld for each calendar year. Generally, U.S. employees are responsible for determining their tax liability based on the amount of wages earned in the tax year and the amount of taxes withheld.

11. SSA is the federal agency responsible for administering retirement, disability, survivor, and family benefits, and enrolling eligible individuals in Medicare. SSA also provides Social Security Numbers, which are unique identifiers needed to work, and a database of which is used to verify employment eligibility by the E-Verify system. Generally, U.S. employers withhold federal social security taxes from the pay checks of their employees and transmit those funds to the United States government. Generally, U.S. employers transmit reports to the SSA of the total wages earned and the total social security taxes withheld for each calendar year. Generally, U.S. employees are eligible for benefits from SSA on the basis of this reported information.

THE CONSPIRATORS

12. Defendant Christina CHAPMAN is a U.S. national, who resided in Minnesota and Arizona.

13. JOHN DOE 1, alias 한지호 Jiho HAN (HAN), was an individual residing overseas who opened accounts with a foreign money service transmitter ("MST") that conducts U.S. dollar transactions through a branch in New York (hereinafter "MST-1"). These accounts were used to

receive payroll funds from U.S. companies associated with laptops that were being hosted at CHAPMAN's residences. HAN would then forward the funds to an individual in the People's Republic of China ("China"). HAN also received funds from CHAPMAN for an overseas IT worker that CHAPMAN first deposited into one of her U.S. financial accounts.

14. JOHN DOE 2, alias 浩然 徐 Haoran XU (XU), was an individual residing overseas who registered for financial accounts with U.S. MSTs. XU provided his name, date of birth, and a Chinese National ID to U.S. MSTs to register for these accounts. XU received money generated through the conspiracy into these accounts, including from CHAPMAN. XU's name and address were also used by CHAPMAN and other coconspirators to receive packages in China, including packages containing laptops for remote work at U.S. companies. XU used two U.S.-based MST accounts, both of which listed his address as Dandong, China, a city on the border with North Korea.

15. JOHN DOE 3, alias 春姬 金 Chunji JIN (JIN), was an individual residing overseas who registered for financial accounts with U.S. MSTs. JIN provided her name, date of birth, and a Chinese National ID to U.S. MSTs to register for these accounts. JIN received money generated through the conspiracy into these accounts, including from CHAPMAN. JIN's name and address were also used by CHAPMAN and other coconspirators to receive packages in China, including packages containing laptops for remote work at U.S. companies. JIN used two U.S.-based MSTs, one of which listed her address as Dandong, China, a city on the border with North Korea.

16. JOHN DOE 4, alias or moniker "Zhonghua," and "Venechor S." (hereinafter "Zhonghua") was a foreign national not authorized to work in the United States. Zhonghua was a manager of other overseas IT workers and had direct communication with CHAPMAN regarding the scheme.

17. At all times relevant to this Indictment, CHAPMAN, HAN, XU, JIN, and Zhonghua knew that the individuals with whom they conspired to obtain remote IT work were foreign nationals not located in the United States, and not authorized to work in the United States.

JURISDICTION AND VENUE

18. Acts and omissions in furtherance of the offenses alleged herein occurred within the District of Columbia. Pursuant to Title 18, United States Code, Section 3237, venue is proper in the District of Columbia.

19. Additionally, certain of the offenses alleged herein were begun and committed outside of the jurisdiction of any particular state or district of the United States. For those offenses, pursuant to Title 18, United States Code, Section 3238, venue is proper in the District of Columbia.

THE CONSPIRACY

20. Beginning at least in or around October 2020, the exact date being unknown to the Grand Jury, through on or about October 26, 2023, CHAPMAN and others known and unknown to the Grand Jury, in the District of Columbia and elsewhere, knowingly combined, conspired, and agreed together and with each other to defraud by means of deceit, craft, trickery, and dishonesty the United States and its agencies, to include:

a. DHS, by submitting false identification information stolen or borrowed from U.S. persons to DHS for employment eligibility verification through the use of the E-Verify system;

b. IRS, by causing U.S. employers to submit false information regarding wages earned by U.S. persons, when in fact those persons did not work for said employers and had their identities stolen or borrowed, and thereafter creating false tax liabilities in the name of the U.S. persons; and

c. SSA, by causing U.S. employers to submit false information regarding benefits earned by U.S. persons, when in fact those persons did not work for said employers and had their identities stolen or borrowed, and thereafter creating false benefit coverage in the name of the U.S. persons.

21. The goals and purposes of the Conspiracy were, among others, to obtain U.S. employment for the overseas IT workers through the use of false, borrowed, or stolen identities in violation of U.S. laws, to generate revenue for the overseas IT workers and their associates, and to generate revenue for CHAPMAN.

Manner and Means

22. It was further a part of the Conspiracy that the coconspirators used the following manner and means, among others, to achieve the goals of the Conspiracy:

a. The overseas IT workers stole the identities of U.S. persons, and otherwise convinced U.S. persons to loan the overseas IT workers their identities for money;

b. The overseas IT workers validated the stolen U.S. person identities by using online background check service providers, under accounts opened, authorized, and paid for by CHAPMAN;

c. The overseas IT workers identified jobs of interest in U.S. companies, including Fortune 500 companies, in fields such as technology, car manufacturing, aerospace, media, retail, and food delivery;

d. The overseas IT workers developed fictitious personas and online profiles to match the job requirements for remote IT worker positions at the U.S. companies and government agencies;

e. The overseas IT workers applied for jobs at the U.S. companies and government agencies, and transmitted false information to DHS as part of an employment eligibility check, to include stolen or borrowed identity information, false drivers' licenses, false Social Security cards, and passports and permanent resident identification cards for individuals other than themselves;

f. CHAPMAN assisted overseas IT workers with transmitting false information and false documents to their employers for the purposes of employment eligibility verification;

g. The overseas IT workers directed the U.S. companies to send their company-issued laptops to CHAPMAN's U.S.-based addresses;

h. CHAPMAN hosted these laptops at her residences, logging into the U.S. companies' networks, sometimes daily, and then permitting the coconspirator overseas IT workers to connect remotely to the laptops;

i. CHAPMAN sent certain of these laptops to the overseas IT workers at locations in China and elsewhere;

j. The overseas IT workers caused the U.S. companies to issue paychecks in the names of stolen, false, and borrowed U.S. person identities, and on numerous occasions, directed those payments to be sent to CHAPMAN's residences;

k. CHAPMAN forged the signature of the false, stolen, or borrowed U.S. person identities on checks sent to her residence and deposited those checks at her bank, U.S. Financial Institution 1 ("USFI-1"); and

l. CHAPMAN, HAN, XU, JIN, and Zhonghua transferred money between and among accounts at U.S. financial institutions and MSTs, which were further

transferred to other conspirators.

Overt Acts

23. In furtherance of this Conspiracy and to accomplish its goals, the following overt acts, among others, were committed in the District of Columbia and elsewhere:

- ***Initiation of the Conspiracy***

a. In or around March 2020, an unknown coconspirator approached CHAPMAN, through her LinkedIn page, and asked her to "be the U.S. face" of their company and assist them in helping the overseas IT workers gain remote employment in the United States.

- ***Targeting of U.S. Companies***

b. Between in or around August 2022, through in or around November 2023, a group of North Korean IT workers stored a set of files related to the scheme in an online repository. These files included documents about attempting to obtain employment in the United States as remote workers, including guides and tips related to topics about writing a cover letter, building a resume, sample resumes, scripts for interviews, and a scanned copy of a stolen U.S. Permanent Resident Card. Included in the documents were 59 job postings, including:

i. A job post for a "Video Streaming Engineer" Company 1, a top-5 national television network and media company, headquartered in New York. As discussed further herein, infra ¶ 23(w), on or about November 21, 2022, a remote IT worker associated with CHAPMAN obtained employment as a video engineer for Company 1's streaming service;

ii. A job post for a "Python Developer" at Staffing Company 1, a

professional staffing company, which staffs contractors at thousands of U.S. companies, headquartered in Florida. As discussed further herein, infra ¶ 23(aa), on or about June 16, 2023, a remote IT worker associated with CHAPMAN, claiming experience in using "Python" software, obtained employment at Staffing Company 1; and

iii. A job post for a "Video Streaming Engineer" at Staffing Company 2, a professional staffing company. As discussed further herein, infra ¶ 23(dd) below, on or about May 17, 2022, a remote IT worker associated with CHAPMAN, obtained employment at Staffing Company 2 for this contract, and was contracted to the Company 3, a Fortune 500 company and one of the most recognizable media and entertainment companies in the world, headquartered in California.

c. Between on or about September 21, 2022, and on or about March 3, 2023, a contractor using the name "Asolelei T." obtained employment at Cyber Security Firm-1 ("CSF-1"), a cyber-security contractor located in California, through a staffing company. "Asolelei T." was a U.S. person identity that was used for remote IT positions that were associated with Chapman's laptop farm. During the time period of his employment, "Asolelei T." used a number of tactics, techniques, and procedures associated with the group of North Korean IT workers identified above, to include remote control web browser extensions to provide remote access to CSF-1's system via proxy services and VPNs to mask his IP address. In addition to "Asolelei T.," eight other contractors associated with this group of North Korean IT workers obtained jobs at CSF-1, all hired

through third-party staffing companies. In total, three of these individuals used U.S. person identities that were also used at CHAPMAN's laptop farm. As described further herein, CHAPMAN invoiced the coconspirator overseas IT workers for services related to two CSF-1 laptops hosted at her laptop farm.

- ***Targeting of U.S. Person Identities***

d. On or about February 25, 2022, a coconspirator registered an account associated with CHAPMAN's name and address with a Maryland-based online background check service provider, Online Background Check Service-1 ("OBCS-1").

e. On or about February 25, 2022, CHAPMAN messaged a coconspirator overseas IT worker identified as "Joren Jo" ("JJ"). CHAPMAN provided JJ with her debit card information, which was used to make payments on an account in CHAPMAN's name with OBCS-1. CHAPMAN told JJ that she would "add the total charge to the invoice."

f. On or about February 25, 2022, a coconspirator created an account at MST-2 (hereinafter "MST-2 Account A"), headquartered in California, using CHAPMAN's identifying information, CHAPMAN's debit card, and an email address for a coconspirator overseas IT worker. Thereafter, MST-2 Account A was used for payments to the OBCS-1 account associated with CHAPMAN.

g. On or about January 20, 2023, CHAPMAN provided information for another of her debit cards to an overseas IT worker, via a messaging application.

h. On or about February 15, 2023, a coconspirator created another MST-2 account (hereinafter "MST-2 Account B") with CHAPMAN's identifying information,

the new debit card, and the email address of a coconspirator overseas IT worker.

i. Between on or about February 25, 2022, and on or about August 2, 2023, coconspirator overseas IT workers used the OBCS-1 account associated with CHAPMAN to conduct more than 80 queries, to include criminal history reports and Social Security Number traces, of the following 57 U.S. persons' identities, verifying their information and Social Security Numbers, in order to further their impersonation of these U.S. persons with U.S. employers:

Sub-¶	U.S. Identity
1	"Aaron L."
2	"Aaron M."
3	"Adrian S."
4	"Andrew C."
5	"Andrew S."
6	"Arion S."
7	"Arkim P."
8	"Arnaldo M."
9	"Breeyan C."
10	"Brett S."
11	"Brian S."
12	"Byron P."
13	"Carol W."
14	"Carol W."
15	"Christopher A."
16	"Christopher H."
17	"Chuck C."
18	"Cole D."
19	"Daniel M."
20	"Darnell M."
21	"Daron T."
22	"Dong C."
23	"Dustin S."
24	"Dustin S."
25	"Gregory J."

26	"Guillermo C."
27	"Jacob L."
28	"Jamal M."
29	"James V."
30	"Jamie M."
31	"Jared G."
32	"Joe C."
33	"JungWoo L."
34	"Justin G."
35	"Justin G."
36	"Kalvim W."
37	"Kelly K."
38	"Kevin S."
39	"Lamar M."
40	"Michael B."
41	"Michael P."
42	"Pheng C."
43	"Pu H."
44	"Richard C."
45	"Ronald Z."
46	"Ruben G."
47	"Scott O."
48	"Shunquez L."
49	"Steven A."
50	"Steven L."
51	"Thomas K."
52	"Thomas K."
53	"Tony C."
54	"Victor C."
55	"Victor K."
56	"Weichong C."
57	"Yu D."

j. Between on or about February 25, 2022, and on or about August 2, 2023, CHAPMAN and her coconspirators paid the fees associated with OBCS-1 accounts in CHAPMAN's name via the following methods:

Sub-¶	Number of Transactions	Total Amount	CHAPMAN Account
1	42	$ 501.20	MST-2 Account A
2	11	$ 115.85	MST-2 Account B
3	27	$ 189.00	USFI-2 Account

k. On or about December 14, 2021, an overseas IT worker registered an account with a California-based online background check service provider, OBCS-2.

l. Between on or about December 14, 2021, and on or about November 14, 2023, coconspirator overseas IT workers used OBCS-2's website to query more than 1,700 U.S. persons' identities, in order to verify their information, including the following 56 stolen U.S. persons' identities which were used in the scheme:

Sub-¶	U.S. Identity
1	"Dong C."
2	"Asolelei T."
3	"Darius P."
4	"Kevin S."
5	"Cody W."
6	"Daniel B."
7	"Brian S."
8	"WeiChong C."
9	"Marcus M."
10	"Jade H."
11	"Sion W."
12	"Kou T."
13	"Ryan F."
14	"James B."
15	"Scott L."
16	"Willy E."

17	"Curtis W."
18	"Royd L."
19	"Steven L."
20	"Nathanael D."
21	"Joseph P."
22	"Michael G."
23	"Breeyan C."
24	"Daniel P."
25	"Kentrell M."
26	"Alexander M."
27	"Jami J."
28	"Justin S."
29	"Matthew L."
30	"Sutton A."
31	"Troy S."
32	"Nathan H."
33	"Randy B."
34	"Raymond S."
35	"Phong T."
36	"Joshua T."
37	"Jerry P."
38	"Michael H."
39	"Charles W."
40	"Michael P."
41	"Michael P."
42	"Pheng C."
43	"Pu H."
44	"Richard C."
45	"Ronald Z."
46	"Ruben G."
47	"Scott O."
48	"Shunquez L."
49	"Steven A."
50	"Steven L."
51	"Thomas K."
52	"Tony C."
53	"Victor C."
54	"Victor K."

55	"Weichong C."
56	"Yu D."

m. Between on or about December 15, 2021, and on or about October 16, 2023, coconspirator overseas actors made payments to OBCS-2 for associated searches using a third MST-2 account controlled by CHAPMAN (hereinafter "MST-2 Account C").

n. On or about September 21, 2023, CHAPMAN messaged with a coconspirator overseas IT worker using the screenname "Chai D.," wherein Chai D. asked CHAPMAN to retrieve a physical badge at Company 5, a Fortune 500 aerospace and defense manufacturer. CHAPMAN said she would send one of her assistants, but noted that "they don't know that you guys use 'borrowed identities'." CHAPMAN asked Chai D. whether he was indeed "Ryan F.," the worker employed at Company 5 who had received a physical badge. Chai D. answered, "no" and CHAPMAN replied, "So it's a stolen identity…And you're asking me to have my assistant handle something that is illegal."

o. On or about October 12, 2023, Chai D. sent CHAPMAN a message related to a payment for CHAPMAN's assistant picking up the Company 5 physical ID. CHAPMAN responded, "That's actually Zhonghua's account. He'll have to send it to me from there."

p. On or about October 12, 2023, CHAPMAN received a payment for $200 from MST-1 from an account with the name of "Venechor S.," an account associated with Zhonghua.

q. On or about November 15, 2022, CHAPMAN messaged with an overseas IT worker using the screenname "Alexander The Great" ("AT"), wherein AT asked

CHAPMAN for assistance creating a background story for a stolen U.S. person identity, "Daniel B." AT noted that the real Daniel B. had a criminal record and employers were asking for more information as to what offenses were committed. CHAPMAN provided a cover story and asked "What information do you know about Daniel B[.]?? Do you know his race?" AT responded that the real Daniel B. was "a black man" but that he (AT) was Asian. AT then gave CHAPMAN his "real full name," which was a Chinese name.

- ***Transmitting False Information to Gain Employment, Including to DHS***

r. On or about the following dates, coconspirator overseas IT workers applied for employment with U.S. companies and caused U.S. companies to transmit false information, to include false information about U.S. persons' identities and false documents to DHS USCIS via the E-Verify system, in order to verify employment eligibility:

Sub-¶	Case Initiated Date	U.S. Person Identity	Document 1	State	Document 2
1	7/1/2021	"Asolelei T."	State Driver's License/ID	CA	Social Security ("SS") Card
2	11/4/2021	"Asolelei T."	State Driver's License/ID	CA	SS Card
3	12/15/2021	"Asolelei T."	State Driver's License/ID	CA	SS Card
4	4/28/2022	"Asolelei T."	State Driver's License/ID	CA	SS Card
5	9/21/2022	"Asolelei T."	State Driver's License/ID	CA	SS Card
6	11/3/2022	"Asolelei T."	State Driver's License/ID	CA	SS Card
7	11/1/2022	"Breeyan C."	State Driver's License/ID	CA	SS Card
8	12/5/2022	"Breeyan C."	State Driver's License/ID	CA	SS Card
9	7/20/2023	"Breeyan C."	State Driver's License/ID	CA	SS Card
10	6/14/2023	"Brian S."	State Driver's License/ID	AL	SS Card
11	3/10/2023	"Chai D."	State Driver's License/ID	TX	SS Card
12	4/18/2022	"Charles C."	State Driver's License/ID	CA	SS Card
13	4/26/2022	"Charles C."	State Driver's License/ID	CA	SS Card

14	6/24/2022	"Charles/Mailee C."	State Driver's License/ID	CA	SS Card
15	9/25/2023	"Cody W."	State Driver's License/ID	AL	SS Card
16	9/26/2023	"Cody W."	State Driver's License/ID	AL	SS Card
17	10/13/2023	"Cody W."	State Driver's License/ID	AL	SS Card
18	10/12/2022	"Daniel B."	State Driver's License/ID	NY	SS Card
19	10/17/2022	"Daniel B."	State Driver's License/ID	NY	SS Card
20	11/15/2022	"Daniel B."	State Driver's License/ID	NY	SS Card
21	5/12/2023	"Darius W."	State Driver's License/ID	SC	SS Card
22	5/15/2023	"Darius W."	State Driver's License/ID	SC	SS Card
23	9/27/2023	"Darius W."	State Driver's License/ID	SC	SS Card
24	10/11/2023	"Darius W."	State Driver's License/ID	SC	SS Card
25	10/19/2023	"Darius W."	State Driver's License/ID	SC	SS Card
26	5/10/2021	"David S."	ID card from U.S. gov. agency	n/a	U.S. birth certificate
27	7/6/2021	"David S."	State Driver's License/ID	GA	Cons Rep of Birth Abroad (FS-240)
28	8/19/2021	"David S."	State Driver's License/ID	GA	Cert of Rep of Birth (DS-1350)
29	11/29/2021	"David S."	ID card from U.S. gov. agency	n/a	Cert of Rep of Birth (DS-1350)
30	1/11/2022	"David S."	State Driver's License/ID	GA	U.S. birth certificate
31	1/14/2022	"David S."	State Driver's License/ID	GA	U.S. birth certificate
32	4/11/2022	"David S."	State Driver's License/ID	GA	U.S. birth certificate
33	4/28/2022	"David S."	State Driver's License/ID	GA	U.S. birth certificate
34	6/10/2022	"David S."	State Driver's License/ID	GA	U.S. birth certificate
35	6/13/2022	"David S."	State Driver's License/ID	GA	U.S. birth certificate
36	7/3/2023	"Dong C."	State Driver's License/ID	TX	SS Card
37	9/18/2023	"Dong C."	State Driver's License/ID	TX	SS Card
38	10/3/2023	"Dong C."	State Driver's License/ID	TX	SS Card
39	11/22/2023	"Dong C."	State Driver's License/ID	TX	SS Card
40	3/23/2022	"Frank A."	State Driver's License/ID	TX	SS Card

41	4/8/2022	"Frank A."	State Driver's License/ID	TX	SS Card
42	6/3/2022	"Frank A."	State Driver's License/ID	TX	SS Card
43	7/13/2022	"Frank A."	State Driver's License/ID	TX	SS Card
44	7/19/2022	"Frank A."	State Driver's License/ID	TX	SS Card
45	7/28/2023	"Frank A."	State Driver's License/ID	TX	SS Card
46	2/21/2022	"Frank C."	State Driver's License/ID	TX	SS Card
47	4/27/2022	"Frank C."	State Driver's License/ID	TX	SS Card
48	3/2/2021	"Guillermo C."	Alien Resident Card	n/a	n/a
49	6/7/2021	"Guillermo C."	Alien Resident Card	n/a	n/a
50	8/26/2021	"Guillermo C."	Alien Resident Card	n/a	n/a
51	5/3/2022	"Guillermo C."	State Driver's License/ID	NV	SS Card
52	5/4/2022	"Guillermo C."	State Driver's License/ID	NV	SS Card
53	5/9/2022	"Guillermo C."	Alien Resident Card	n/a	n/a
54	5/11/2022	"Guillermo C."	State Driver's License/ID	NV	SS Card
55	5/11/2022	"Guillermo C."	State Driver's License/ID	NV	SS Card
56	5/20/2022	"Guillermo C."	State Driver's License/ID	NV	SS Card
57	5/23/2022	"Guillermo C."	State Driver's License/ID	NV	SS Card
58	10/5/2022	"Guillermo C."	State Driver's License/ID	NV	SS Card
59	10/20/2022	"Guillermo C."	State Driver's License/ID	NV	SS Card
60	3/23/2023	"Jack W."	U.S. Passport/Passport Card	n/a	n/a
61	12/28/2021	"Jacob L."	State Driver's License/ID	CA	SS Card
62	7/7/2022	"Jacob L."	State Driver's License/ID	CA	SS Card
63	9/7/2023	"Jade H."	State Driver's License/ID	MI	SS Card
64	10/18/2023	"Jade H."	State Driver's License/ID	MI	SS Card
65	5/18/2023	"James B."	State Driver's License/ID	PA	SS Card
66	7/11/2023	"James B."	State Driver's License/ID	PA	SS Card
67	8/22/2023	"James B."	State Driver's License/ID	PA	SS Card
68	2/8/2022	"Jungwoo L."	State Driver's License/ID	AR	SS Card
69	2/8/2022	"Jungwoo L."	State Driver's License/ID	AR	SS Card
70	2/8/2022	"Jungwoo L."	State Driver's License/ID	AR	SS Card
71	2/8/2022	"Jungwoo L."	State Driver's License/ID	AR	SS Card
72	2/8/2022	"Jungwoo L."	State Driver's License/ID	AR	SS Card
73	2/8/2022	"Jungwoo L."	State Driver's License/ID	AR	SS Card
74	2/9/2022	"Jungwoo L."	Alien Resident Card	n/a	n/a
75	12/30/2022	"Kevin S."	State Driver's License/ID	SC	SS Card
76	1/23/2023	"Kevin S."	State Driver's License/ID	SC	SS Card
77	3/17/2023	"Kevin S."	State Driver's License/ID	SC	SS Card

78	6/26/2023	"Kevin S."	State Driver's License/ID	SC	SS Card
79	9/27/2021	"Lee Y."	State Driver's License/ID	CA	SS Card
80	12/3/2021	"Lee Y."	State Driver's License/ID	CA	SS Card
81	2/17/2022	"Lee Y."	State Driver's License/ID	CA	SS Card
82	4/28/2022	"Lee Y."	State Driver's License/ID	CA	SS Card
83	5/6/2022	"Lee Y."	State Driver's License/ID	CA	SS Card
84	6/28/2022	"Lee Y."	State Driver's License/ID	CA	SS Card
85	7/26/2022	"Lee Y."	State Driver's License/ID	CA	SS Card
86	8/11/2022	"Lee Y."	State Driver's License/ID	CA	SS Card
87	8/23/2022	"Lee Y."	State Driver's License/ID	CA	SS Card
88	8/29/2022	"Lee Y."	State Driver's License/ID	CA	SS Card
89	9/1/2022	"Lee Y."	State Driver's License/ID	CA	SS Card
90	10/18/2022	"Lee Y."	State Driver's License/ID	CA	SS Card
91	10/24/2022	"Lee Y."	State Driver's License/ID	CA	SS Card
92	11/1/2022	"Lee Y."	State Driver's License/ID	CA	SS Card
93	9/19/2022	"Marcus M."	State Driver's License/ID	MN	SS Card
94	9/27/2022	"Marcus M."	State Driver's License/ID	MN	SS Card
95	3/14/2023	"Marcus M."	U.S. Passport/Passport Card	n/a	n/a
96	11/1/2023	"Marcus M."	State Driver's License/ID	MN	SS Card
97	3/21/2023	"Matthew R."	State Driver's License/ID	FL	SS Card
98	4/4/2023	"Matthew R."	State Driver's License/ID	FL	SS Card
99	11/14/2022	"Michael G."	State Driver's License/ID	PA	SS Card
100	6/28/2023	"Nathanael D."	State Driver's License/ID	NY	SS Card
101	6/5/2023	"Ryan F."	State Driver's License/ID	MD	SS Card
102	8/2/2023	"Ryan F."	State Driver's License/ID	MD	SS Card
103	8/2/2023	"Ryan F."	State Driver's License/ID	MD	SS Card
104	9/14/2023	"Ryan F."	State Driver's License/ID	MD	SS Card
105	4/13/2022	"Salem O."	U.S. Passport/Passport Card	n/a	n/a
106	7/25/2023	"Sion W."	State Driver's License/ID	CA	SS Card
107	1/30/2023	"Steven L."	State Driver's License/ID	AL	SS Card

s. Between on or about April 22, 2022, and on or about April 26, 2022, CHAPMAN messaged with a coconspirator overseas IT worker using the screenname "Max," wherein they discussed CHAPMAN assisting in submitting

a Form I-9 to a U.S. company for the U.S. person identity "Weichong C.":

> Max: So we need to send envolop [sic] to any USPS location to receive the equipment. I want you to print the following forms and sign with my name and sent it to them. Please help me, Christina.
> [MEDIA ITEM: Label-Weichong C.pdf]
> [MEDIA ITEM: I-9 Electronic Blank.pdf] . . . .
>
> CHAPMAN: Your I-9 didn't come through properly. I can't print it out. . . .
>
> CHAPMAN: I finally got it printed. I will copy the information tomorrow and get it sent out.
>
> Max: Got it[] Got it. . . . Please ship out the hand signed I-9 form by the end of the day" The company send message again. Could you please help me today?
>
> CHAPMAN: Yes. I'll get it out today. . . . I did my best to copy your signature.
>
> Max: haha. Thank you.
>
> CHAPMAN: Your paperwork got sent out today.

t. On or about August 2, 2023, CHAPMAN had a group messaging conversation that included several coconspirator overseas IT workers, in which CHAPMAN acknowledged the severity of falsifying employment eligibility forms (i.e., the Form I-9). Specifically, CHAPMAN stated, "In the future, I hope you guys can find other people to do your physical I9s. These are federal documents. I will SEND them for you, but have someone else do the paperwork. I can go to FEDERAL PRISON for falsifying federal documents."

u. Between on or about August 28, 2023, and on or about August 29, 2023, CHAPMAN messaged with a coconspirator overseas IT worker using the screenname "Chong," wherein they discussed CHAPMAN's assistance in transmitting false identity documents to a U.S. employer for employment

eligibility verification:

> Chong: I received an offer from [Company 55] . . . . [C]ould you please print two documents on paper and deliver to NY? . . . It's not a card, it's a paper. The temporary DL card. Can you help me with that? . . . Because I can't make a valid DL card, I said that I had lost my DL card. The company provided another option – I can do the drug test with the temporary DL card in my hand. So I have to find another person who can do the drug test with the document once you print them. I checked by online research for [sic] several times and it's said that the temporary DL card doesn't have barcode or hologram. And it can be printed by myself as well. So I think it's possible as long as you can print them for me. [W]hat is your thought?
>
> CHAPMAN: If I'm just printing and sending. . . .
>
> Chong: Great. . . .
> [MEDIA ITEM: image:2023_08_28T18_47_34_462Z.png]
> Just one more thing, is this the right form of Alabama temporary DL card? Do you have any of idea?
>
> CHAPMAN: I guess. It's the same image I get when I Google.
>
> Chong: Thanks. . . . Hi Christina. Please print follow documents.
> [MEDIA ITEM: Drug Screen Registration.pdf]
> [MEDIA ITEM: Stephen Kyle C[]TemporaryDL.pdf]
> [MEDIA ITEM: Clinic Authorization Form – AOH C[].pdf]
> Please print them and send to this address – [Address] Brooklyn NY.
> Please share tracking number once you've finished. . . .
>
> CHAPMAN: Just waiting for a pick up [sic].

- ***Employment in United States Through CHAPMAN's Laptop Farm & Other Assistance***

v. On or about the following dates, coconspirator overseas IT workers obtained employment and performed remote IT work for U.S. companies, while the laptops provided for this work were hosted by CHAPMAN at a laptop farm in one of her residences:

Sub-¶	Start Date	U.S. Person Identity	Victim Company (if known)	Staffing Company (if applicable)	Total Wages (if known)
1	7/5/2022	"Asolelei T."	Company 10		$156,826.00
2	5/31/2023	"Brian S."	Company 11		$88,061.00
3	6/12/2023	"Brian S."	Company 12	Staffing Company 10	
4	4/14/2022	"Charles C."		Staffing Company 11	$208,562.00
5	9/26/2023	"Cody W."	Company 13		$7,269.92
6	9/25/2023	"Cody W."	Company 14	Staffing Company 12	
7	4/17/2023	"Curtis W."	Company 7	Staffing Company 15	
8	5/1/2023	"Curtis W."	Company 15	Staffing Company 13	
9	4/30/2023	"Danie P."	Company 16		
10	11/21/2022	"Daniel B."	Company 1		$121,213.00
11	10/31/2022	"Daniel B."	Company 17		$3,889.00
12	10/31/2022	"Daniel B."	Company 18		
13	5/31/2023	"Darius W."	Company 19		
14	10/31/2023	"Darius W."		Staffing Company 11	$11,011.00
15	5/15/2023	"Darius W."	Company 20		$67,084.00
16	4/7/2022	"David S."	Company 4	Staffing Company 3	$86,778.00
17	10/3/2023	"Dong C."	Company 21	Staffing Company 14	$8,568.00
18	9/18/2023	"Dong C."		Staffing Company 9	$8,639.00
19	3/21/2022	"Dung N."		Staffing Company 16	$101,646.35
20	4/14/2022	"Frank C."	Multiple, including Company 6	Staffing Company 5	$214,596.00
21	8/7/2023	"Frank C."	Company 7	Staffing Company 6	$40,320.00
22	7/18/2022	"Frank C."	Company 22	Staffing Company 17	$115,248.00
23	3/31/2023	"Frank C."	Company 23		

24	5/9/2022	"Guillermo C."	Company 24	Staffing Company 3	$41,175.00
25	5/23/2022	"Guillermo C."	Company 25	Staffing Company 33	$81,004.00
26	4/20/2023	"Guillermo C."	Company 26		
27	5/11/2022	"Guillermo C."	Company 27	Staffing Company 18	$17,150.00
28	11/5/2022	"Irving B."	Company 28	Staffing Company 19	$60,551.22
29	9/5/2023	"Jade H."	Company 29		$23,017.00
30	10/16/2023	"Jade H."	Company 30		
31	1/4/2023	"Jamal M."	Company 31		
32	7/24/2023	"James B."	Company 32	Staffing Company 31	$14,400.00
33	5/26/2022	"JungWoo L."		Staffing Company 16	$9,135.00
34	1/30/2023	"Kentrell M."	Company 33		
35	1/31/2023	"Kentrell M."	Company 34	Staffing Company 32	
36	6/16/2023	"Kevin S."	Company 2	Staffing Company 1	$35,815.00
37	10/18/2021	"Kou T."	Company 35	Staffing Company 20	
38	10/17/2022	"Lee Y."	Company 36		$3,553.34
39	6/27/2022	"Lee Y."	Company 37		
40	8/29/2022	"Lee Y."	Company 38		$130,661.07
41	10/24/2022	"Lee Y."	Company 39		
42	9/30/2022	"Marcus M."	Company 40		
43	3/20/2023	"Marcus M."	Company 9	Staffing Company 3 and Staffing Company 27	
44	9/26/2022	"Marcus M."	Company 41		$9,225.00
45	1/17/2022	"Matthew L."	Company 42	Staffing Company 5	
46	5/31/2022	"Matthew L."	Company 43		
47	4/3/2023	"Matthew R."	Company 44		$76,923.00
48	4/26/2023	"Royd L."		Staffing Company 8	

49	8/2/2023	"Ryan F."	Company 5	Staffing Company 4	$36,586.00
50	7/31/2023	"Ryan F."	Company 45	Staffing Company 21	$31,777.00
51	9/18/2023	"Ryan F."	Company 46		
52	6/6/2022	"Ryan S."		Staffing Company 3	
53	4/11/2022	"Salem O."	Company 47		$83,620.00
54	4/25/2023	"Scott L."	Company 48		$81,250.00
55	6/26/2023	"Scott L."	Company 49		
56	7/24/2023	"Sion W."		Staffing Company 7	$24,378.00
57	4/8/2022	"WeiChong C."	Company 50		$234,840.00
58	7/19/2022	"William P."	Company 51	Staffing Company 22	$63,280.00
59	10/2/2023	"Willy E."	Company 7	Staffing Company 22	
60	11/30/2022	Unknown	Company 52		
Total					$2,298,051.90

Company 1

w. On or about November 21, 2022, a coconspirator overseas IT worker using the U.S. identity "Daniel B." obtained a job at Company 1 for a remote position as a software engineer for Company 1's digital streaming service, see supra ¶ 23(b)(i). The coconspirator overseas IT worker provided CHAPMAN's address to Company 1's Human Resources department as his permanent residence.

x. On or about November 16, 2022, CHAPMAN received a package addressed to "Daniel B." containing a laptop for his employment at Company 1. CHAPMAN affixed a hand-written note with the name of "Daniel B." and Company 1 on the laptop.

y. On November 21, 2022, CHAPMAN messaged with coconspirator AT, wherein they discussed CHAPMAN's assistance with setting up the laptop for AT to work at Company 1. After running through the process of getting the laptop set up for use (to include exchanging log-in credentials for the laptop), CHAPMAN installed AnyDesk, a remote login application, and stated:

> CHAPMAN: This computer SHOULD have been loaded with the necessary software. Can you control?
>
> AT: Yes, I can control. [Company 1] Anydesk is not available, I think it's probably screen lock issue. Could you please remove Anydesk and install it again inside download? and please unlock screensavor [sic] forever. . . .
>
> AT: Hi, please help me, it's very urgent. I have to meet team in 30 mins.

CHAPMAN then responded to AT and helped with the AnyDesk re-download.

z. Between on or about November 22, 2023, and on or about November 23, 2023, CHAPMAN had further messages with AT about technical assistance for the Company 1's laptop:

> AT: Could you follow these for [Company 1]'s laptop? I can not [sic] do these by myself because it requires to do restart. . . .
>
> AT: We are going to have laptop setup meeting in 20 mins. Can you join Teams meeting and follow what IT guy say? Because it will require to restart laptop multiple times and I can not [sic] handle that. You can mute and just follow what they say, they have access to entire screen and will control of most of things without you. However, you have to restart it inevitably . . . .
>
> AT: You can join Teams meeting from your phone or your own laptop. . . .
>
> CHAPMAN: Who do I say I am?
>
> AT: You don't have to say, I will be joining there too.
>
> CHAPMAN: It's going to have my name on it, right?
>
> AT: You just mute and listen, then follow what she instruct, she may ask you

to restart laptop. . . .

CHAPMAN: I just typed in the name Daniel. If they ask WHY you are using two devices, just say the microphone on your laptop doesn't work right.

AT: Ok

CHAPMAN: Most IT people are fine with that explanation.

Company 2 / Staffing Company 1

aa. On or about June 16, 2023, a coconspirator overseas IT worker using the U.S. identity "Kevin S." obtained a position at Staffing Company 1 for a remote position as a software engineer. The resume for "Kevin S." included a list of skills to include "Python," a programming software, see supra ¶ 23(b)(ii).

bb. On or about July 17, 2023, "Kevin S." began a contractor assignment at Company 2, a health care administration company located in Missouri.

cc. On or about July 13, 2023, CHAPMAN received a package addressed to "Kevin S." at her residence, which included a Company 2 laptop for remote work. CHAPMAN affixed a hand-written note with the name of "Kevin S." and Company 2's name on the laptop.

Company 3 / Staffing Company 2

dd. On or about May 17, 2022, CHAPMAN exchanged communications with a user listed as "Mobile & Web Projects" ("M&W") related to a laptop for a job contracted through Staffing Company 2, see supra ¶ 23(b)(iii). M&W told CHAPMAN that a laptop would soon be arriving from Company 3 / Staffing Company 2 and to "ping me" when it arrived.

ee. On or about May 19, 2022, CHAPMAN confirmed that the Company 3 / Staffing Company 2 laptop had arrived.

ff. On or about May, 20 2022, CHAPMAN and M&W messaged about the setup process for this laptop, to include installing AnyDesk.

Company 4 / Staffing Company 3

gg. On or about April 7, 2022, a coconspirator overseas IT worker using the U.S. identity "David S.," who had obtained employment at a staffing company, Staffing Company 3, was assigned to a remote position at Company 4, a Fortune 500 Silicon Valley technology company. CHAPMAN received a Company 4 laptop for "David S." at her residence and maintained it there.

hh. On or about April 11, 2022, CHAPMAN messaged with a coconspirator overseas IT worker using the screenname "BH." BH asked, "Any laptop was delivered under 'David S.'?" CHAPMAN responded that it had arrived. BH wrote, "I want to access that remotely You know how to install Anydesk?" CHAPMAN responded, "I do it practically EVERYDAY!" CHAPMAN then installed AnyDesk and set up the laptop for remote work. BH later confirmed that the set up worked and he was able to control the laptop remotely.

Company 5 / Staffing Company 4

ii. On or about August 2, 2023, a coconspirator overseas IT worker using the U.S. identity "Ryan F.," who had obtained employment at Staffing Company 4, a staffing company, was assigned to a remote position at Company 5. CHAPMAN received a Staffing Company 4 laptop at her residence.

jj. On or about September 26, 2023, Company 5 sent a company-issued laptop to "Ryan F." to CHAPMAN's residence, which had a PIV card, issued by Company 5 in the name of "Ryan F.", associated with it.

Company 6 / Staffing Company 5

kk. On or about April 14, 2022, a coconspirator overseas IT worker using the U.S. identity "Frank C." obtained a remote IT position at a staffing company, Staffing Company 5.

ll. On or about February 6, 2023, "Frank C.," still being employed by Staffing Company 5, was contracted to Company 6, a Fortune 500 iconic American automotive manufacturer located in Detroit, Michigan.

mm. Between on or about February 6, 2023, and on or about February 8, 2023, CHAPMAN messaged with an individual referred to as "Web Dev" ("WD"), regarding the delivery of the Company 6 laptop.

nn. On or about February 8, 2023, CHAPMAN received a shipment addressed to "Frank C." at CHAPMAN's residence, which included a laptop for remote work at Company 6. CHAPMAN affixed a hand-written note with "Frank C.'s" name and log-in information on the laptop.

oo. On or about February 14, 2023, WD and CHAPMAN messaged about the Company 6 laptop:

> WD: And could we do the computer setup for [Company 6] company computer?. . . And could we connect my [Company 6] computer zoom to Steve's apple computer zoom link? (Because apple computer zoom is no use so I am gonna use it for [Company 6] computer)
>
> please join [Company 6] computer to this zoom.
> Meeting Link: *** *** 5266
> Passcode: ****xc
>
> CHAPMAN: I created a second desktop on [Company 6] for zoom, just in case.
>
> WD: Cool. How did you pass this step? What admin username and password did you use? This one I mean.

> CHAPMAN: I rarely have issues installing Zoom in computers. . . . Anydesk is what required an admin username and password, not Zoom.
>
> WD: Oh. I got it. . . . And for [Company 6] compute[sic], it is showing zoom controlling alert now. . . .That seems due to my developer joined. . . . Anyway to hide it in my way?
>
> CHAPMAN: Controlling alert.

Company 7 / Staffing Company 6

pp. On or about August 1, 2023, a coconspirator overseas IT worker using the U.S. identity "Frank C." obtained employment with a staffing company, Staffing Company 6, and was contracted for a remote IT position at Company 7, a Fortune 500 high-end retail store with multiple U.S. locations.

qq. On or about July 27, 2023, CHAPMAN messaged with an individual referred to as "Project Manager" ("PM"), about the laptop for Company 7 being delivered to CHAPMAN's address.

rr. On or about July 31, 2023, CHAPMAN received a shipment to "Frank C." at CHAPMAN's residence, which included a Company 7 laptop for remote work. CHAPMAN affixed a hand-written note with the name "Frank C." and "Company 7."

ss. On or about August 3, 2023, after the laptop arrived at CHAPMAN's residence, CHAPMAN and PM argued over a messaging application about whether CHAPMAN would set up the laptop that day, given her prior promises to set up laptops for other overseas IT workers:

> CHAPMAN: I didn't say setup should be today. . . . I'll tell the other people who start TOMORROW morning, that Yuri says he's more important . . . . Will they know you are Yuri over there?

PM: Let me know who is planed [sic] for today, I will have a talk with them. Yes.

CHAPMAN: Because I don't know who is on who's team, or who know about each other… I can't reveal other names. I got some people in trouble for that before.

Company 8

tt. On or about October 16, 2023, a coconspirator overseas IT worker using the U.S. identity "Darius W." obtained a remote software engineer position at Company 8, a restaurant chain headquartered in Michigan. As a software engineer, "Darius W." had access to sensitive segments of Company 8 servers. "Darius W." requested the Company 8 laptop be sent to CHAPMAN's residence.

uu. On or about October 24, 2023, "Darius W." took leave, claiming that his father had fallen ill. He did not return to work following his absence and continued his unpaid leave.

vv. Between on or about October 16, 2023, and on or about November 9, 2023, "Darius W." accessed and downloaded large amounts of information from Company 8 servers.

Company 9

ww. Beginning on or about March 20, 2023, a coconspirator overseas IT worker using U.S. identity "Marcus M.," who had obtained employment at a staffing company, was contracted to Company 9, a classic American clothing brand headquartered in California, for a remote position. Company 9 sent a shipment to "Marcus M." at CHAPMAN's residence, which included a laptop for remote work.

xx. Between on or about September 9, 2023, and on or about October 4, 2023, "Marcus M.," caused what appeared to be 15 separate exfiltrations of data from IP addresses, which appeared to resolve to a location in Nigeria.

Attempts at U.S. Government Agencies

yy. On or about June 29, 2023, a coconspirator overseas IT worker using the U.S. identity "Sion W." obtained employment at Staffing Company 7, a staffing company, to work in a contractor remote position with the DHS Immigration and Customs Enforcement ("ICE"), a U.S. Government Agency located in the District of Columbia. "Sion W." provided CHAPMAN's residence as the home address on the DHS paperwork. Subsequently, on or about October 24, 2023, Staffing Company 7 HR staff reached out to "Sion W." stating that they needed to speak about "identity issues" and needed "Sion W.'s" birth certificate or passport. DHS/ICE required fingerprints be submitted for its contractor positions. "Sion W." did not submit fingerprints, was not verified to work as a contractor for DHS/ICE.

zz. On or about April 25, 2023, a coconspirator overseas IT worker using the U.S. identity "Royd L." obtained employment at Staffing Company 8, a staffing company, to work in a contractor remote position with DHS Federal Protective Service ("FPS"). "Royd L." listed CHAPMAN's address on his application for employment with Staffing Company 8. Subsequently, on or about April 27, 2023, DHS/FPS provided "Royd L." forms and instructions necessary for "Royd L." to complete his background check for the contractor position, including information for scheduling a required fingerprint examination.

aaa. On or about May 3, 2023, "Royd L." informed Staffing Company 8 that he had a death in the family and would not be available for a week.

bbb. On or about May 8, 2023, "Royd L." informed Staffing Company 8 that he was quitting the job due to the need to stay to support his family.

ccc. On or about September 27, 2023, a coconspirator overseas IT worker using the U.S. identity "Dong C.," who had obtained employment at a staffing company, Staffing Company 9, was contracted for a remote IT position to the General Services Administration ("GSA"), a U.S. Government Agency located in the District of Columbia. "Dong C." provided CHAPMAN's address as his home address to the staffing company and listed "Christina" as his "spouse."

ddd. On or about September 27, 2023, "Dong C." virtually attended a GSA staff meeting but was unable to communicate besides introducing himself. Thereafter, he attended several other meetings without speaking and was otherwise unable to be reached. On or about October 2, 2023, GSA staff made the determination to terminate "Dong C." as a contractor.

Other Assistance Provided by CHAPMAN to Overseas IT Workers

eee. On or about February 25, 2022, CHAPMAN provided technical assistance to coconspirator overseas IT workers over messaging applications. CHAPMAN messaged with Zhonghua about logging into a laptop. CHAPMAN attempted to log into the laptop using the username and password that Zhonghua provided to her. CHAPMAN told Zhonghua that they had already tried to log in using those login credentials. Zhonghua asked her to try it again and CHAPMAN sent an image of a laptop screen which showed the username or password was

incorrect and told Zhonghua, "We are locked out again. Please verify."

fff. On or about March 24, 2022, CHAPMAN messaged with Zhonghua, wherein Zhonghua requested CHAPMAN's assistance in obtaining an IRS Wage and Tax Statement (a Form W-2 or "W-2") for a coconspirator overseas IT worker "Matthew" and sought samples of W-2s as it was "really important for our work."

ggg. On or about the following dates, CHAPMAN furthered the Conspiracy by sending laptops and other devices issued by U.S. companies to the following overseas locations, to facilitate remote work at U.S. companies, including to Dandong, China, a city on the border with North Korea:

Sub-¶	Date	Receiver Name	Receiver Location	Shipment Description
1	12/9/2022	JIN	Dandong, China	Laptops - Computer Laptop
2	12/9/2022	JIN		Laptops - Computer Laptop
3	12/16/2022	JIN		Laptops - Work Laptop. Not
4	12/16/2022	JIN		Laptops - Work Laptop. Not
5	12/20/2022	IT Worker 1		Laptops - 1 Used Apple Laptop
6	12/20/2022	IT Worker 1		Laptops - 1 Used Apple Laptop
7	12/20/2022	IT Worker 1		Laptops - 1 Used Apple Laptop
8	12/23/2022	JIN		Laptops - Used Laptop
9	12/23/2022	JIN		Laptops - Used Laptop
10	12/23/2022	JIN		Laptops - Used Laptop
11	1/12/2023	XU		Computer
12	1/12/2023	XU		Computer
13	1/12/2023	JIN		Computer
14	1/12/2023	JIN		Computer
15	1/18/2023	JIN		Phone
16	1/18/2023	JIN		Phone
17	2/6/2023	JIN		Computer
18	2/6/2023	JIN		Computer
19	2/22/2023	JIN		Computer

20	2/22/2023	JIN	Dandong, China	Computer
21	3/16/2023	JIN		Used Samsung Tablet USB AC ADA
22	3/16/2023	JIN		Used Samsung Tablet USB AC ADA
23	3/16/2023	XU		Refurbished Samsung Galaxy Mob
24	3/16/2023	XU		Refurbished Samsung Galaxy Mob
25	4/1/2023	XU		Computer
26	4/1/2023	XU		Computer
27	4/6/2023	IT Worker 2	Karachi, Pakistan	
28	4/6/2023	IT Worker 3	Yanji City, China	Company 16 TV Stick
29	4/6/2023	IT Worker 3		Company 16 TV Stick
30	4/10/2023	XU	Dandong, China	Computer
31	4/10/2023	XU		Computer
32	4/19/2023	JIN		Cell Phones - 2 Used Cell
33	4/19/2023	JIN		Cell Phones - 2 Used Cell Phon
34	5/2/2023	IT Worker 4	Shenyang, China	Used Macbook Computer
35	5/2/2023	IT Worker 4		Used Macbook Computer
36	5/3/2023	IT Worker 5	Karachi, Pakistan	Computer
37	5/13/2023	IT Worker 6	Dubai, UAE	Computer
38	5/13/2023	IT Worker 6		Computer
39	5/18/2023	IT Worker 7	Karachi, Pakistan	
40	5/30/2023	IT Worker 8	Abuja, Nigeria	Computer
41	5/31/2023	IT Worker 8		Laptops - Laptop, Not for Re S
42	6/13/2023	IT Worker 9	Dandong, China	Mac Laptop
43	6/13/2023	IT Worker 9		Mac Laptop
44	7/8/2023	JIN		Laptops - 2 Used Laptops. Not
45	7/19/2023	XU		Laptops - 1 Laptop for business
46	7/19/2023	XU		Laptops - 1 Laptop for business
47	7/22/2023	IT Worker 7	Karachi, Pakistan	Laptops - 1 Laptop For business
48	8/29/2023	IT Worker 10	Shenyang, China	Computer - New Mac Apple
49	8/29/2023	IT Worker 10		Computer - New Mac Apple

- ***Transmission of False Employment Data to IRS and SSA***

hhh. Between on or about January 1, 2022, and on or about January 31, 2024, the coconspirators caused U.S. companies to transmit false wage and tax information on more than 100 occasions to the SSA and the IRS for the wages earned by the overseas IT workers under the scheme, in the name of the following U.S. persons, when those U.S. persons did not in fact earn such wages and which the U.S. companies did not know was associated with stolen or borrowed U.S. identities:

Sub-¶	U.S. Person	2021 Wages	2022 Wages	2023 Wages	Total False Wages Reported
1	"Asolelei T."	$62,137.00	$486,728.00	$265,911.00	$814,776.00
2	"Breeyan C."		$21,280.00	$56,973.00	$78,253.00
3	"Brett S."		$28,110.00	$94,865.00	$122,975.00
4	"Brian S."			$88,061.00	$88,061.00
5	"Charles C."		$106,444.00	$114,280.00	$220,724.00
6	"Chuck C."	$103,444.00	$183,212.00		$286,656.00
7	"Cody W."		$9,053.00	$41,520.00	$50,573.00
8	"Daniel B."		$40,396.00	$114,320.00	$154,716.00
9	"Daniel M."		$1,457.00	$27,691.00	$29,148.00
10	"Darius W."			$176,296.00	$176,296.00
11	"David S."	$160,580.00	$403,640.00		$564,220.00
12	"Dong C."		$22,037.00	$26,347.00	$48,384.00
13	"Dustin S."		$23,539.00	$22,582.00	$46,121.00
14	"Frank C."	$12,183.00	$468,463.00	$471,463.00	$952,109.00
15	"Guillermo C."	$202,161.00	$409,005.00		$611,166.00
16	"Jack W."			$11,592.00	$11,592.00
17	"Jacob L".		$150,569.00	$17,508.00	$168,077.00
18	"Jade H."			$23,017.00	$23,017.00
19	"James B."			$43,782.00	$43,782.00
20	"Jared G."	$32,015.00	$10,707.00	$19,639.00	$62,361.00
21	"Joseph P."			$67,265.00	$67,265.00
22	"JungWoo L."		$85,802.00		$85,802.00
23	"Kevin S."			$195,093.00	$195,093.00

24	"Lamar M."			$8,249.00	$8,249.00
25	"Marcus M."		$81,173.00	$211,403.00	$292,576.00
26	"Matthew R."		$70,329.00	$88,043.00	$158,372.00
27	"Michael G."		$46,996.00	$9,497.00	$56,493.00
28	"Michael P."		$9,511.00		$9,511.00
29	"Nathanael D."			$1,103.00	$1,103.00
30	"Ruben G."			$4,419.00	$4,419.00
31	"Ryan F."			$119,034.00	$119,034.00
32	"Salem O."		$83,620.00		$83,620.00
33	"Shunquez L."	$23,138.00	$75,500.00	$75,500.00	$174,138.00
34	"Sion W."			$24,378.00	$24,378.00
35	"Steven L."			$112,262.00	$112,262.00
36	"Tavaris B."			$115,180.00	$115,180.00
37	"Thomas K."		$1,153.00		$1,153.00
38	"WeiChong C."		$131,889.00	$129,873.00	$261,762.00
	Totals	$595,658.00	$2,950,613.00	$2,777,146.00	$6,323,417.00

(Conspiracy to Defraud the United States, in violation of Title 18, United States Code, Section 371)

COUNT TWO
(Conspiracy to Commit Wire Fraud)

24. The allegations in Paragraphs 1 through 23 of this Indictment are incorporated and re-alleged by reference herein.

25. Between in or around March 2021, until on or about October 26, 2023, CHAPMAN and others known and unknown to the Grand Jury, in the District of Columbia and elsewhere, knowingly combined, conspired, and agreed together and with each other to devise and intended to devise a scheme to defraud U.S. company employers and DHS through the transmission of false information, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing the scheme described above, and attempting to do so, caused to be transmitted by means of wire communication in

interstate commerce the signals and sounds as described in Count One.

(**Conspiracy to Commit Wire Fraud**, in violation of Title 18, United States Code, Sections 1343 & 1349)

COUNT THREE
(Conspiracy to Commit Bank Fraud)

26. The allegations in Paragraphs 1 through 23 of this Indictment are incorporated and re-alleged by reference herein.

27. Between on or about November 30, 2021, until on or about October 26, 2023, CHAPMAN and others known and unknown to the Grand Jury, in the District of Columbia and elsewhere, knowingly combined, conspired, and agreed together and with each other to execute and attempt to execute a scheme and artifice (i) to defraud a financial institution, as defined in 18 U.S.C. § 20; and (ii) to obtain money, funds, credits, assets, securities, and other property owned by and under the custody and control of, a financial institution as defined in 18 U.S.C. § 20, by means of false and fraudulent pretenses, representations, and promises, *to wit*, by impersonating U.S. persons, forging check endorsements, and causing U.S. companies to make deposits in the names of individuals who were falsely associated with the transactions, and thereby causing the banks to unknowingly process transactions to or for the benefit of foreign individuals and entities, including North Korea.

28. In furtherance of this Conspiracy and to accomplish its goals, the following overt acts, in addition to those previously alleged, among others, were committed in the District of Columbia and elsewhere:

Fraud Directed Toward USFI-3

29. On or about November 30, 2021, CHAPMAN messaged with a coconspirator overseas IT worker using the screenname "Piety," wherein they discussed a scheme to deposit

wages into CHAPMAN's account at USFI-3, an FDIC-insured U.S. financial institution, and submit false information to the bank related to the same:

> CHAPMAN: You are Jerry P[.], correct?
>
> Piety: Yes.
>
> CHAPMAN: What's should I do about your payroll check that came here? . . . Where was your check supposed to go?. . .
>
> Piety: was it shipped to your house? . . .
>
> CHAPMAN: Yes. That's why I have it. Sometimes, if you don't have your direct deposit paperwork in quickly enough, the very first check won't make it in to three bank. I'm not sure how to get out to you. . . .WHERE is your bank? . . . I should be able to write your bank account number on the check and send it to your bank then it will be deposited.
>
> Piety: . . . [USFI-3 Name, Address, Routing, Account Information]
>
> CHAPMAN: Okay. I should be able to deposit your check at any [USFI-3] then. Awesome!! That issue is solved.
>
> Piety: how do you handle it?
>
> CHAPMAN: I will write ' For deposit only to account [number] where the signature would go and give it to the teller. . . . Are you there?!?!! I'm at the bank now with your check. Is the account in your name? I need to know.
>
> Piety: hi. No. 1 sec.
>
> CHAPMAN: What name is on the account?? I need to know.
>
> Piety: Anastasiia [D.] it's owner name . . .

Fraud Directed Toward USFI-1

30. On or about June 28, 2022, CHAPMAN messaged with a coconspirator overseas IT worker JJ, wherein they discussed a scheme to deposit checks for overseas IT workers' wages into CHAPMAN's account at USFI-1, an FDIC-insured U.S. financial institution, and submit false information to the bank related to the same:

> JJ: Is it possible to use your bank account for getting payment from one of the company? . . .
>
> CHAPMAN: I'm working on finding out what kind of bank account I need to do that without issue though.
>
> JJ: This is a new company so you don't need to worry about having trouble. I only need to get payment with your bank account once or twice. Meanwhile, I will create my own account and change it.
>
> CHAPMAN: And do you know what happens when my bank account gets flagged by the federal government for processing to many large payments and sending them overseas? I get in trouble and go to prison. I have to make sure I am doing it the right way. . . .
>
> JJ: I totally understand your concern. Sorry to bother you.
>
> CHAPMAN: It's okay. I'm waiting on answers form a bank manager to make sure I can do it without getting in trouble. It will just take a couple days to find out.

31. On or about March 17, 2023, CHAPMAN messaged with a coconspirator overseas IT worker using the screenname "WebHamster" ("WH"), wherein they discussed a scheme to deposit checks for overseas IT workers' wages into CHAPMAN's account at USFI-1 and submit false information to the bank related to the same:

> WH: They are saying they sent another paper check on 2/3, any paper check you received? and would you find someone who can help with physical paper checks, i will pay 30% fee, if needed. the problem is that "Irving B." isn't real person's name. it would be great if you could spare me just a few mins to discuss about the paper checks.
>
> CHAPMAN: That's probably why it didn't go through my bank as the name is fake. I could go to prison for fraud for that. . . . So, Irving is not a real person at all?
>
> WH: No. any possibility? . . .
>
> CHAPMAN: I am willing to try one more time. But I don't have another check. A second one never came here.
>
> WH: I will check with the company, but you could try with the one which be arrived soon. It will be about 3.8k. and 30% will be paid as fee.

32. On or about the following dates, after endorsing the check issued in the name of a beneficiary other than herself and signing the check for deposit, CHAPMAN deposited the following payroll checks into her USFI-1 account via the bank's mobile deposit feature:

Sub-¶	Date of Check	Date of Deposit	U.S. Company	Pay To Order	Amount
a.	9/15/2022	9/27/2022	Company 54	"Lee Y."	$ 3,328.58
b.	9/15/2022	9/30/2022	Company 54	"Lee Y."	$ 4,886.26
c.	9/30/2022	10/11/2022	Company 54	"Lee Y."	$ 4,886.27
d.	1/27/2023	3/6/2023	Staffing Company 34	"Guillermo C."	$ 2,367.34
e.	2/9/2023	3/24/2023	Staffing Company 28	"Frank A."	$ 4,175.23
f.	3/15/2023	3/28/2023	Company 28 - Staffing Company 19	"Irving B."	$ 3,840.17
g.	3/31/2023	4/12/2023	Company 28 - Staffing Company 19	"Irving B."	$ 3,840.08
h.	4/3/2023	4/25/2023	Staffing Company 29	"Lee Y."	$ 2,179.53
i.	3/6/2023	5/1/2023	Staffing Company 30	"Asolelei T."	$ 4,551.65
j.	4/11/2023	5/17/2023	Company 1	"Daniel B."	$ 4,379.36
k.	5/15/2023	5/19/2023	Company 28 / Staffing Company 19	"Irving B."	$ 3,840.17
l.	4/13/2023	6/7/2023	Company 28 / Staffing Company 19	"Irving B."	$ 3,899.65
m.	2/28/2023	6/12/2023	Company 53	"Matthew R."	$ 960.44
n.	5/31/2023	6/20/2023	Company 28 / Staffing Company 19	"Irving B."	$ 3,840.09
o.	6/16/2023	7/6/2023	Company 1	"Daniel B."	$ 4,713.87
p.	7/20/2023	8/3/2023	Staffing Company 27	"Marcus M."	$ 3,264.00
q.	6/27/2023	8/14/2023	Staffing Company 15	"Kentrell M."	$ 2,318.19
				Total	$ 61,270.88

Fraud Directed Toward USFI-2

33. Between on or about October 5, 2023, and on or about October 6, 2023, CHAPMAN messaged with a coconspirator overseas IT worker using the screenname "Tommy," wherein they discussed a scheme to deposit wages into CHAPMAN's account at USFI-2, an FDIC-insured U.S. financial institution, and submit false information to the bank related to the same:

> CHAPMAN: I haven't heard a single word from you today. I needed to give the bank that information today. . . .
>
> Tommy: Could you please let me know your phone number.
> I need to know your phone number at least while bank calls me.
>
> CHAPMAN: 763-[XXX-XXXX].
>
> Tommy: No worries. You only helped your friend Andy. . . .
>
> CHAPMAN: You have to say that we've met in person and worked together. . . . You ABSOLUTELY have to say we've met and worked together. And I won't be able to use this account again for your direct deposit. This bank said it's against their rules.

34. On or about October 11, 2023, CHAPMAN continued the conversation with "Tommy" related to the scheme to deposit wages into CHAPMAN's account at USFI-2:

> CHAPMAN: They can't use the number you gave me because it's a V[oice] O[ver] IP number. They need a physical regular number that is tied to his name and comes up WITH his name. . . .
>
> Tommy: Okay. Let me know your another [sic] [MST-2] address. I will pay. I have just checked with Andy. . . .As you know, Andy has only VOIP phone right now because he was Chineese [sic] guy. . . .or can you tell me bank assist's number please? . . .then we will let [Company 56] manager who is real call bank assist and confirm. . . .
>
> CHAPMAN: The bank said only Andy, calling from a real number can confirm that the money was meant to go into my account. . . .
>
> Tommy: then we can prepare one of my US friend. he has real US number and can pretend to be Andy. I will provide all information about Andy to him. What do you think?

> CHAPMAN: It HAS to be in the name Andy P[.]. . . .
>
> Tommy: Make sense. You mean the real phone number which I will give you should be connected name which is Andy P[.]? I think it's impossible . . . .
>
> CHAPMAN: Your friend here needs to go get a sim card, saying he's buying it for his friend Andy P[.] so it gets put in his name. If the bank asks about the new number, he can just say he moved recently. Then that sim card can be put in an extra phone for the phone call/s. I told the bank that I usually talked to Andy via [Messaging Application-1] because it was easier as we moved and traveled for work. Alternatively, your friend can get a Lan line in Andy's name. You guys obviously have a social security number for him. That would be registered in his name.
>
> Tommy: Ok. Let me try.

35. On or about October 13, 2023, "Tommy" relayed to CHAPMAN that they had purchased a phone with a Subscriber Identity Module ("SIM") card in "Andy's" name, and that they were "preparing" a "story."

36. Between on or about October 15, 2023, and on or about October 19, 2023, CHAPMAN continued the conversation with "Tommy" related to the scheme to deposit wages into CHAPMAN's account at USFI-2:

> Tommy: 385[XXXXXXX]. This is phone number. I will let you know when he is ready to answer. Let's confirm again. Andy and you are friends and have worked some stuffs in person. Andy had some issues about bank so made a decision to use your bank. Right?
>
> CHAPMAN: Yes. We worked together in person before and became friends... so I offered to help when he mentioned his bank issue.
>
> Tommy: Okay.
>
> CHAPMAN: I'll call the bank tomorrow. That department isn't open this late. . . .
>
> Tommy: Did you call the bank btw?
>
> CHAPMAN: Yes. I've called. Have they contacted your friend yet?

> Tommy: Not yet.
>
> CHAPMAN: I'll call again tomorrow. . . .
>
> CHAPMAN: I'm losing my account and no longer eligible to have accounts at [USFI-2]. There will be a balance owed because I already sent you money. The ONLY thing that can fix this is Andy P[.] going into a [USFI-2] location and showing his idea and saying he asked to have his money deposited into my account. . . .
>
> Tommy: I will prepare my friends to visit at the [USFI-2] with Andy's id. . . .
>
> CHAPMAN: We need someone who looks like Andy.
>
> Tommy: I will let andy [sic] call first and if it didn't go well, will let company manager call the bank. if it's also not going well, we can choose the third way.

37. On or about the following dates, Company 50 made direct deposits for wages of coconspirator overseas remote IT workers into CHAPMAN's USFI-2 account, which were falsely attributed to a U.S. person:

Sub-¶	Company 50 Deposit Date	Identity Used	Deposit Amount
a.	4/20/2022	"Weichong C."	$1,751.60
b.	05/19/2022	"Weichong C."	$8,662.14
c.	06/02/2022	"Weichong C."	$4,331.12
d.	06/16/2022	"Weichong C."	$4,331.14
e.	06/30/2022	"Weichong C."	$4,331.12
f.	07/14/2022	"Weichong C."	$4,331.14
		Total	$27,738.26

(**Conspiracy to Commit Bank Fraud**, in violation of Title 18, United States Code, Sections 1344(1) & (2), 1349)

COUNT FOUR
(Aggravated Identity Theft)

38. The allegations in Paragraphs 1 through 37 of this Indictment are incorporated and re-alleged by reference herein.

39. Between in or around October 2020, and on or about October 26, 2023, CHAPMAN and others known and unknown to the Grand Jury, within the District of Columbia and elsewhere, knowingly transferred, possessed, and used, without lawful authority, a means of identification of another person during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), *to wit* conspiracy to commit wire fraud and conspiracy to commit bank fraud as set forth in Counts Two and Three, knowing that the means of identification belonged to another actual person, including the use of identities defined in ¶¶ 23(r), 32-34, 37.

(**Aggravated Identity Theft**, in violation of Title 18, United States Code, Sections 2, 1028A(a)(1))

COUNT FIVE
(Conspiracy to Commit Identity Fraud)

40. The allegations in Paragraphs 1 through 37 of this Indictment are incorporated and re-alleged by reference herein.

41. Between in or around October 2020, and on or about October 26, 2023, CHAPMAN and others known and unknown to the Grand Jury, within the District of Columbia and elsewhere, knowingly combined, conspired, and agreed together and with each other to transfer, possess, and use, in or affecting interstate or foreign commerce, without lawful authority, a means of identification of another person, namely, the names, Social Security numbers, and dates of birth of the stolen or borrowed U.S. person identities, with the intent to commit, and to aid and abet, in connection with, unlawful activity that constitutes a violation of Federal law and that constitutes a felony under applicable State and local law, namely, conspiracy to commit wire fraud

and bank fraud, as described in Counts Two and Three, and as a result of the offense, CHAPMAN and the conspirators obtained something of value aggregating $1,000 or more during any 1-year period.

(**Conspiracy to Commit Fraud and Related Activity in Connection with Identification Documents**, in violation of Title 18, United States Code, Sections 1028(a)(7), (b)(1)(D), (c)(3)(A), & (f))

COUNT SIX

(Conspiracy to Launder of Monetary Instruments)

42. The allegations in Paragraphs 1 through 37 of this Indictment are incorporated and re-alleged by reference herein.

43. Between in or around October 2020, until on or about October 26, 2023, defendants CHAPMAN, HAN, XU, and JIN, and others known and unknown to the Grand Jury, within the District of Columbia and elsewhere, knowingly combined, conspired, and agreed together and with each other to conduct financial transactions affecting interstate and foreign commerce, *to wit,* transfers from accounts at USFI-1, USFI-2, MST-2, and MST-3, to accounts at MST-2, MST-3, and MST-1, which involved the proceeds of a specified unlawful activity, that is conspiracy to commit wire fraud, conspiracy to commit bank fraud, and conspiracy to commit identity fraud, as described in Counts Two, Three, and Five, knowing that the transaction was designed in whole and in part to conceal and disguise, the nature, location, source, ownership, and control of the proceeds of said specified unlawful activity and that while conducting and attempting to conduct such financial transaction knew that the property involved in the financial transaction represented the proceeds of some form of unlawful activity.

- ***Incoming Funds from U.S. Companies Transferred to MST Accounts***

44. On or about the following dates, CHAPMAN received payroll wages for coconspirator overseas IT workers from U.S. companies directly deposited into her USFI-2

account, and then transferred those funds into XU's account at MST-3, headquartered in New York, including as follows:

Sub-¶	Payroll Deposit Date	Payroll Deposit Amount	Transfer Date to MST-3	Transfer Amount
a.	4/20/2022	$1,751.60	4/28/2022	$1,750.84
b.	5/19/2022	$8,662.14	5/23/2022	$8,662.14
c.	6/2/2022	$4,331.12	6/4/2022	$4,331.12
d.	6/16/2022	$4,331.14	6/18/2022	$4,331.14
e.	6/30/2022	$4,331.12	7/5/2022	$4,331.00
f.	7/14/2022	$4,331.14	7/15/2022	$4,330.00
			Total	$23,406.24

45. In addition, coconspirator overseas IT workers from U.S. companies directly deposited funds into CHAPMAN's USFI-1 account, and then transferred those funds into HAN's account at MST-1, operating in New York.

Sub-¶	Payroll Deposit Date	Payroll Deposit Amount	Transfer Date to MST-1	Transfer Amount
a.	9/15/2022	$ 3,328.58	9/28/2022	$544.00
b.	9/15/2022	$ 4,886.26	10/3/2022	$4856.26
c.	9/30/2022	$ 4,886.27	10/14/2022	$4856.27
			Total	$10,256.53

46. Between on or about January 15, 2021, and on or about October 26, 2023, approximately $990,248.84 was deposited into HAN's account at MST-1 from various U.S. companies, including those whose laptops were operated at CHAPMAN's laptop farm at her residences, and the money thereafter transferred out to other MST-1 accounts.

- ***Money Paid by Overseas IT Workers for CHAPMAN's Services Via MSTs***

47. On or about February 28, 2022, CHAPMAN messaged with Zhonghua, wherein he directed CHAPMAN to send an invoice to him. CHAPMAN did send a "February 2022 Invoice" which showed fees related to 15 different identities working for 17 different listed U.S. companies.

Zhonghua then wrote, "and from next month, we will pay the money via [MST-3]. How do you think about this?" CHAPMAN responded, "That sounds good. The feds here are now tracking every penny on [MST-2], [MST-4], etc. They aren't doing that on [MST-3] yet."

48. On or about the following dates, CHAPMAN charged coconspirator overseas IT workers for "rent" and other fees for the services that she rendered in operating the laptop farm, to include logging into the U.S. companies' laptops, connecting to the U.S. companies' networks, connecting the overseas IT workers remotely to the laptops, providing technical support with the connections, storage of the laptops, and shipping laptops:

Sub-¶	Approximate Date	Amount
a.	11/30/2021	$2,832.00
b.	12/31/2021	$3,586.00
c.	1/31/2022	$3,601.00
d.	2/28/2022	$4,325.00
e.	3/31/2022	$6,556.00
f.	4/30/2022	$8,179.00
g.	5/31/2022	$11,731.00
h.	6/30/2022	$10,688.00
i.	7/31/2022	$12,464.00
j.	8/31/2022	$9,515.00
k.	9/30/2022	$10,001.00
l.	10/31/2022	$5,170.00
m.	11/30/2022	$9,369.00
n.	12/31/2022	$8,561.00
o.	1/31/2023	$7,453.00
p.	2/28/2023	$8,778.00
q.	3/31/2023	$4,459.00
r.	4/30/2023	$7,920.00
s.	5/31/2023	$4,698.00
t.	6/30/2023	$7,642.50
u.	7/31/2023	$7,847.50
v.	8/31/2023	$2,175.50
w.	9/30/2023	$9,179.50
x.	10/31/2023	$10,119.00
	Total	$176,850.00

49. Between in or around March 2021, and in or around March 2023, XU's MST-2 account sent CHAPMAN's MST-2 Account A 90 transfers totaling approximately $142,919.00. Most of the transfers contained notes that referenced "Service Fee," "Shipment Fee," "Development Work," "Web Design," "Purchase Computer," Equipment Purchase," and "HTML Design."

50. Between on or about December 14, 2021, and on or about April 3, 2023, JIN's MST-2 account sent CHAPMAN's MST-2 Account A nine transfers totaling approximately $12,210.00. Most of the transfers contained notes that referenced "Service Fee" or "Shipment Fee."

51. Between in or around September 2021, and in or around June 2023, CHAPMAN transferred $153,857 from her MST-2 Account to her USFI-2 account.

(**Conspiracy to Launder of Monetary Instruments**, in violation of Title 18, United States Code, Sections 1956(a)(1)(B)(i) & (h))

COUNT SEVEN

(Prohibition of Unlicensed Money Transmitting Business)

52. The allegations in Paragraphs 1 through 51 of this Indictment are incorporated and re-alleged by reference herein.

53. Between in or around October 2020, until on or about October 26, 2023, within the District of Columbia and elsewhere, CHAPMAN and others known and unknown to the grand jury did knowingly conduct, control, manage, supervise, direct and own all and part of an unlicensed money transmitting business, which affected interstate and foreign commerce, while failing to comply with the money transmitting business registration requirements under 31 U.S.C. § 5330, or regulations prescribed under that section, and aided and abetted the same.

(**Prohibition of Unlicensed Money Transmitting Business**, in violation of Title 18, United States Code, Sections 1960(a), 2)

COUNT EIGHT

(Conspiracy to Cause the Unlawful Employment of Aliens)

54. The allegations in Paragraphs 1 through 51 of this Indictment are incorporated and re-alleged by reference herein.

55. Between in or around October 2020, until on or about October 26, 2023, CHAPMAN and other coconspirators known and unknown to the Grand Jury, within the District of Columbia and elsewhere, knowingly combined, conspired, and agreed together and with each other to commit a crime against the United States, namely, violations of 8 U.S.C. § 1324a, *to wit* the hiring, recruiting, and referring for a fee aliens, that is coconspirator overseas IT workers for employment in the United States, knowing that said aliens were not authorized for employment in the United States, with respect to such employment.

(**Conspiracy to Cause Unlawful Employment of Aliens**, in violation of Title 18, United States Code, Section 371 and Title 8, United States Code, Section 1324a(a)(1)(A) and 1324a1324A(f)(1))

FORFEITURE ALLEGATION

56. The allegations contained in Counts One through Eight of this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeitures pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c).

57. Pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), upon conviction of violations of Title 18, United States Code, Sections 1028, 1343, 1344, defendant CHAPMAN shall forfeit to the United States of America any property, real or personal, which constitutes or is derived from proceeds traceable to said violation(s). The United States will also seek a forfeiture money judgment for a sum of money equal to the value of any property, real or personal, which constitutes, or is derived from proceeds

traceable to this offense. The property to be forfeited includes, but is not limited to, the following:

a. Funds in CHAPMAN's accounts, as follows:

Sub-¶	Financial Institution	Amount	Identifier
1	USFI-2	$9,767.08	Act. No. *6710
2	USFI-1	$2,117.47	Act. No. *0368

b. Wages and monies accrued by overseas IT workers, as follows:

Sub-¶	Seized From	Identity Used	Identifier	Amount
1	Company 32	"James B."	Technical Consultant - PO-0005486	$6,400.00
2	Company 50	"WeiChong C."	SSN *8146	$9,007.73
3	Company 29	"Jade H."	SSN *6658	$1,292.12
4	Company 36	"Lee Y."	SSN *2245	$3,553.34
5	Company 10	"Asolelei T."	SSN *8216	$6,889.60
6	Staffing Company 11	"Charles C."	SSN *2658	$5,115.38
7	Company 1	"Daniel B."	SSN *9074	$23,569.37
8	Company 10	"Asolelei T."	SSN *8216	$4,904.55
9	Company 46	"Ryan F."	SSN *7992	$5,970.61
10	Company 53	"Matthew R."	SSN *7198	$7,198.52
11	MST-1	JIHO HAN	Membership No. *7044	$6,072.47
12	Company 28	"Irving B."	SSN *3338	$2,124.71
13	Company 14	"Cody W."	SSN *2295	$1,825.99
14	Payroll Company 1/ Company 48	"Scott L."	SSN *5106	$9,473.63
15	Staffing Company 11	"Charles C."	SSN *2658	$7,235.70
16	Staffing Company 23	"Frank A."	SSN *0908	$16,155.15
17	Staffing Company 24	"James B."	SSN *9838	$3,541.20
18	Staffing Company 25	"Dong C."	SSN *3852	$8,907.16
19	Staffing Company 26	"Dong C."	SSN *3852	$6,956.00

c. All fees, payments, and monies derived from services performed on behalf of the conspiracy.

58. The allegations contained in Counts One through Eight of this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeitures pursuant to

Title 18, United States Code, Sections 982(a)(1).

59. Pursuant to Title 18, United States Code, Section 982(a)(1), upon conviction of an offense in violation of Title 18, United States Code, Sections 1956 & 1960, defendants CHAPMAN, XU, HAN, and JIN shall forfeit to the United States of America any property, real or personal, involved in such offense, and any property traceable to such property. The United States will also seek a forfeiture money judgment for a sum of money equal to the value of any property, real or personal, which constitutes, or is derived from proceeds traceable to this offense. The property to be forfeited includes, but is not limited to, the following:

a. Funds in CHAPMAN's accounts, as follows:

Sub-¶	Financial Institution	Amount	Identifier
1	USFI-2	$9,767.08	Act. No. *6710
2	USFI-1	$2,117.47	Act. No. *0368

b. Wages and monies accrued by overseas IT workers, as follows:

Sub-¶	Seized From	Identity Used	Identifier	Amount
1	Company 32	"James B."	Technical Consultant - PO-0005486	$6,400.00
2	Company 50	"WeiChong C."	SSN *8146	$9,007.73
3	Company 29	"Jade H."	SSN *6658	$1,292.12
4	Company 36	"Lee Y."	SSN *2245	$3,553.34
5	Company 10	"Asolelei T."	SSN *8216	$6,889.60
6	Staffing Company 11	"Charles C."	SSN *2658	$5,115.38
7	Company 1	"Daniel B."	SSN *9074	$23,569.37
8	Company 10	"Asolelei T."	SSN *8216	$4,904.55
9	Company 46	"Ryan F."	SSN *7992	$5,970.61
10	Company 53	"Matthew R."	SSN *7198	$7,198.52
11	MST-1	JIHO HAN	Membership No. *7044	$6,072.47
12	Company 28	"Irving B."	SSN *3338	$2,124.71
13	Company 14	"Cody W."	SSN *2295	$1,825.99
14	Payroll Company 1/ Company 48	"Scott L."	SSN *5106	$9,473.63

15	Staffing Company 11	"Charles C."	SSN *2658	$7,235.70
16	Staffing Company 23	"Frank A."	SSN *0908	$16,155.15
17	Staffing Company 24	"James B."	SSN *9838	$3,541.20
18	Staffing Company 25	"Dong C."	SSN *3852	$8,907.16
19	Staffing Company 26	"Dong C."	SSN *3852	$6,956.00

c. All fees, payments, and monies involved in services performed on behalf of the conspiracy.

60. If any of the property described above, as a result of any act or omission of a defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty,

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b)(1) and Title 28, United States Code, Section 2461(c).

A TRUE BILL

FOREPERSON

Matthew M. Graves /SMH

Attorney of the United States in
and for the District of Columbia

AO 91 (Rev. 08/09) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

District of Columbia

United States of America
v.
OLEKSANDR DIDENKO,
also known as "Alexander Didenko"
[redacted]

Defendant(s)

Case: 1:24-mj-00152
Assigned to: Judge Upadhyaya, Moxila A.
Assign Date: 4/29/2024
Description: COMPLAINT W/ ARREST WARRANT

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of January 2018 through April 29, 2024 in the county of _____ in the _____ District of Columbia, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 371	- Conspiracy to Defraud the United States and its Agencies
18 U.S.C. §§ 1343 & 1349	- Wire Fraud and Conspiracy
18 U.S.C. § 1028A	- Aggravated Identity Theft
18 U.S.C. §§ 1028(a)(7), (b)(1)(D),(c)(3)(A) & (f)	- Fraud with Identity Documents and Conspiracy
8 U.S.C. § 1324a & 18 U.S.C. §§ 2, 371	- Unlawful Employment of Aliens and Conspiracy
18 U.S.C. §§ 1956(a)(1)(B)(i) & (h)(a)(2)(A), & (h);	- Money Laundering and Conspiracy
18 U.S.C. § 1960	- Unlicensed Money Transmitting Business

This criminal complaint is based on these facts:

See attached Affidavit which is incorporated by reference as if fully stated herein.

❒ Continued on the attached sheet.

Complainant's signature

David Booth, Special Agent, FBI
Printed name and title

Attested to the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1. by telephone, this _____ day of April, 2024.

Date: 04/29/2024

Judge's signature

City and state: Washington, D.C. Moxila A. Upadhyaya, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR AN ARREST WARRANT

I, David Booth, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), currently assigned to the FBI New York Field Office. I have been a Special Agent with the FBI since April 2021. Since that time, I have been involved in national security investigations. Specifically, I have been involved in investigations involving counterintelligence, wire fraud, money laundering, and cybercrime. During my work with the FBI, I have participated in the execution of multiple search warrants, including warrants to search electronic messaging and email accounts.

2. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

3. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that, between approximately January 2018 until the present day, multiple violations of, *inter alia*, 18 U.S.C. § 371 (conspiracy to defraud the United States), 18 U.S.C. §§ 1343 & 1349 (wire fraud and wire fraud conspiracy), 18 U.S.C. § 1028A (aggravated identity theft), 18 U.S.C. § 1028(a)(b) (identity fraud), 8 U.S.C. § 1324a (employment of unauthorized alien in the United States), 18 U.S.C. § 1956(h) (money laundering conspiracy), and 18 U.S.C. § 1960 (unlicensed money transmitting business) have been committed by OLEKSANDR DIDENKO and other known and unknown coconspirators.

II. JURISDICTION AND VENUE

4. This Court has jurisdiction to issue the requested warrant because it is a "court of competent jurisdiction" as defined by 18 U.S.C. § 2711. Specifically, the Court is a "district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). As discussed more fully below, acts or omissions in furtherance of the offenses under investigation occurred within Washington, DC. *See* 18 U.S.C. § 3237.

5. Additionally, certain of the offenses alleged herein were begun and committed outside of the jurisdiction of any particular state or district of the United States. For those offenses, pursuant to Title 18, United States Code, Section 3238, venue is proper in the District of Columbia.

III. STATUTES AND BACKGROUND

A. Relevant Criminal Statutes

6. Under 18 U.S.C. § 371, it is illegal for "two or more persons [to] conspire . . . to commit any offense against the United States," to include fraud on the United States and its agencies.

7. Under 18 U.S.C. § 1343 it is illegal "to devise[] or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice." Under 18 U.S.C. § 1349, it is illegal to conspire to commit offenses under § 1343.

8. Under 18 U.S.C. § 1028A it is illegal to "transfer[], possess[], or use[], without lawful authority, a means of identification of another person" in relation to commission of

another felony, to include violation of 18 U.S.C. § 1343 (wire fraud).

9. Under 18 U.S.C. §§ 1028(a)(7), (b)(1)(D), (c)(3)(A) & (f), it is illegal for any person to "knowingly transfer, possess, or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law," and conspire to do the same.

10. Under 8 U.S.C. § 1324a, "it is unlawful for a person or other entity to hire, or to recruit or refer for a fee, for employment in the United States an alien knowing the alien is an unauthorized alien."

11. Under 18 U.S.C. § 1956 it is illegal to, "knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conduct or attempt to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity . . . knowing that the transaction is 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 specified unlawful activity;." 18 U.S.C. § 1956(a)(1)(B)(i). It is also illegal to "transport[], transmit[], or transfer[], or attempt[] to transport, transmit, or transfer a monetary instrument or funds from a place in the United States to or through a place outside the United States or to a place in the United States from or through a place outside the United States . . . with the intent to promote the carrying on of specified unlawful activity," to include violation of 18 U.S.C. § 1343 (wire fraud) and 18 U.S.C. § 1028(a) (identity theft). 18 U.S.C. § 1956(a)(2)(A). Under 18 U.S.C. § 1956(h), it is illegal to conspire to commit offenses under § 1956.

B. U.S. Government Agencies

12. The Department of Homeland Security (DHS), U.S. Citizenship and Immigration Services (USCIS) is the federal agency responsible for ensuring employment eligibility for workers in the United States. DHS and USCIS are located in the District of Columbia.

a. Federal law requires that every U.S. employer who recruits, refers for a fee, or hires an individual for employment in the United States must complete Form I-9, Employment Eligibility Verification. A Form I-9 must be completed for every individual hired for employment in the United States, including citizens and noncitizens. On the form, an employee must attest to their employment authorization. The employee must also present their employer with acceptable documents as evidence of identity and employment authorization. The employer must examine these documents to determine whether they reasonably appear to be genuine and relate to the employee, then record the document information on the employee's Form I-9. Employers must have a completed Form I-9, Employment Eligibility Verification, on file for each person on their payroll (or otherwise receiving remuneration) who is required to complete the form.

b. As a voluntary alternative to the Form I-9 process, employers may use E-Verify, a web-based system run by USCIS that compares information from Form I-9 to government records to confirm that an employee is authorized to work in the United States. In the E-Verify process, employers create cases based on information taken from an employee's Form I-9, Employment Eligibility Verification. E-Verify then electronically compares that information to records available to DHS and the Social Security Administration. E-Verify generates a response to the employer confirming

the employee's employment eligibility or indicating that the employee needs to take further action to complete the case. Although E-Verify requires the use of a photographic identity document, it does not have the ability to query state drivers' license photographs against the state drivers' license databases.

c. Prior to August 2023, U.S. employers were generally required to review employment eligibility documents in person. After August 2023, employers could remotely examine and submit the employment eligibility documentation through E-Verify.

13. The Internal Revenue Service (IRS) is the federal agency responsible for collection of taxes from U.S. employers and employees. IRS is located in the District of Columbia. Generally, U.S. employers withhold federal taxes from the pay checks of their employees and transmit those funds to the United States government. Generally, U.S. employers transmit to IRS reports of the total wages earned and the total taxes withheld for each calendar year. Generally, U.S. employees are responsible for determining their tax liability based on the amount of wages earned in the tax year and the amount of taxes withheld.

14. The Social Security Administration (SSA) is the federal agency responsible for administering retirement, disability, survivor, and family benefits, and enrolling eligible individuals in Medicare. SSA also provides Social Security Numbers, which are unique identifiers needed to work, and a database of which is used to verify employment eligibility by the E-Verify system. Generally, U.S. employers withhold federal social security taxes from the pay checks of their employees and transmit those funds to the United States government. Generally, U.S. employers transmit to SSA reports of the total wages earned and the total social security taxes withheld for each calendar year. Generally, U.S. employees are eligible for benefits from SSA on the basis of this reported information.

IV. PROBABLE CAUSE

15. The United States is investigating **OLEKSANDR DIDENKO**, also known as "Alexander Didenko" (DIDENKO), a Ukrainian national, last known to reside in Kyiv, Ukraine, as well as identified and unidentified co-conspirators, for a scheme in which persons are fraudulently obtaining employment with U.S.-based companies for monetary gain through use of U.S.-based websites and companies, and illegally using the U.S. financial system in furtherance of the same. As further explained here, financial records of DIDENKO show transactions related to the scheme as early as January 2018, and through the present day.

A. Background

16. UpWorkSell is a business that purports to provide services to remote Information Technology (IT) workers. UpWorkSell uses a publicly-available website, https://upworksell.com (UpWorkSell). I have reviewed the UpWorkSell website, which advertises the ability for remote IT workers to buy or rent accounts in the name of identities other than their own on various online freelance IT job search platforms. Freelance platforms advertised on UpWorkSell include "U.S. Platform-1",[1] located in California, "U.S. Platform-2", located in Pennsylvania, and "Overseas Platform-1," located abroad. These platforms have internet websites that generally allow users to advertise thereon as "gig" workers, *i.e.*, to create free accounts, advertise their skills, and bid on IT work contracts. Generally, money for a contract is held in escrow by the platform and released as payment as the IT worker meets contract

[1] U.S. Platform-1's terms of service state that by registering for an account, the user represents that they are doing business under their own name. Users agree not to provide false or misleading information about their identity or location, or about the beneficial owner(s) of their business.

milestones. The UpWorkSell website also advertises "Credit Card Rental" in the European Union and the United States, SIM card rental for cellular phones, and the ability to buy or rent accounts at online Money Service Transmitters (MST) located in the United States and abroad. Thus, the UpWorkSell website appears to advertise a full array of services to allow an individual to pose under a false identity and market themselves for remote IT work.

17. UpWorkSell is operated by DIDENKO. The UpWorkSell website lists the following "Contact" information: (1) email address [redacted]@gmail.com ("Subject Account-1"); and (2) Telegram handle [redacted] Subscriber records received for Subject Account 1 listed email address [redacted]@gmail.com ("Subject Account-2") and phone number +[redacted]5089 ("Subject Phone Number-1") as the recovery methods for "Subject Account-1". U.S. Department of State records for a May 2023 visa application for DIDENKO show that DIDENKO listed Subject Account-2 and Subject Phone Number-1 as his contact information. Additionally, business records of a U.S. MST located in New York ("MST-2"). for an account belonging to DIDENKO show that Subject Account-2 and Subject Phone Number-1 are listed as the primary methods of contact.

18. As explained further herein, evidence collected during the investigation reveals that DIDENKO manages as many as approximately 871 proxy identities, provides proxy accounts for 3 freelance IT hiring platforms, and provides proxy accounts for 3 different MSTs. In coordination with co-conspirators, DIDENKO facilitates the operation of at least 3 U.S.-based

"laptop farms"[2] hosting approximately 79 computers. DIDENKO's 3 MST accounts, which he uses to send and receive funds in furtherance of the scheme, have received approximately $920,000 in U.S.D. payments since July 2018.

Services Provided by Didenko

19. DIDENKO provides access to proxy financial accounts, including online MSTs based in California ("U.S. MST-1"), New York ("U.S. MST-2"), and overseas ("Overseas MST-1"). Based on my review of the websites for these institutions, these MSTs operate on the internet and permit users to send and receive funds and have access to the U.S. financial system without having to open an account at a brick-and-mortar bank. U.S. MST-2 and Overseas MST-1 offer virtual bank accounts connected to the U.S. financial system and the ability to transfer funds internationally. I know from my experience in this and other investigations that having such accounts allows remote workers to receive payments from U.S.-based employers domestically, and thus can give them the appearance of being located in the United States, obfuscating their true location.

20. UpWorkSell's website also offers to create "credit cards" and then rents the use of those cards to his customers. Based on a review of records from a court-authorized search of DIDENKO's email, the customer sends money to DIDENKO to be loaded onto the card. DIDENKO then provides the card information to the customer after taking a pre-determined amount as a usage fee.

---

[2] As described further herein, a laptop farm is a location in the United States used by remote IT workers to host computers provided to them by employers, in order to create the appearance that the remote IT workers are physically located at the laptop farm address.

21. Based on a review of records from a court-authorized search of DIDENKO's "Online Message Provider-1" account chats ("Subject Account-3") , DIDENKO also offers customers, for a fee, the ability to access freelance worker accounts and the above-mentioned financial accounts via a remote computer desktop program. Email records indicate that DIDENKO's associates operate "laptop farms" in several countries, to include the United States. At these locations, DIDENKO's associates receive computers from the business by whom the remote IT workers are hired and keep them connected to the internet. DIDENKO provides clients (the IT workers) with credentials to remotely log in to these computers. The Internet Protocol ("IP") addresses associated with these computers will resolve to the "laptop farm" location, allowing the remote IT worker to appear as if they are physically located within the country in which they are allegedly working.

22. Based on my training and experience, companies will often block IP addresses that are known to belong to sanctioned countries or proxy services like Virtual Private Networks (VPNs).

23. Based on my training and experience, an individual may seek the services DIDENKO offers on UpWorkSell because he/she would not otherwise be able to obtain freelance IT employment if he/she registered for freelance job websites and financial accounts by disclosing his/her true identity and true location.

24. DIDENKO sells the use of real identities, which may be those of witting or unwitting individuals. A court-authorized search of DIDENKO's email (Subject Account-2) revealed a spreadsheet listing approximately 871 identities linked to accounts with U.S. Platform-1, Overseas Platform-1, and U.S. MST-2 . The search also revealed folders containing photos of passports, driver's licenses, bank statements, and other identity documents. Many of

these photos depict an individual holding their identity document and a handwritten sign with a date. Based on my training and experience these types of documents and photos are often required to verify accounts on the above-mentioned platforms (and thus the individuals in the photos are likely witting participants in the scheme). Additionally, multiple documents in Subject Account-2 appear to be interview scripts with answers to interview questions that are commonly asked via U.S. Platform-1's video verification process.

25. Witting participants who are renting out their identities through DIDENKO are used to coordinate video job interviews on behalf of DIDENKO's customers. For example, a review of Online Message Provider-1 messages from a court-authorized search of Subject Account-3 shows that, in January 2020, DIDENKO had an exchange with an unidentified customer ("Customer-1") in which Customer-1 asked DIDENKO to create an Overseas Platform-1 account and asked if, "Female can do video interview with some clients?" "I mean, she can manage the interview with her technical skills?" DIDENKO responded, "usually not" "they can just talk" "you write – they answer". Later in the conversation, DIDENKO wrote, "we can create a second guy profile if you want. He knows English well and can help with client interviews . . . . [Y]ou will have to pay for each such interview, but he is a good guy."

U.S.-Based Co-Conspirators and "Laptop Farms"

26. As described above, a laptop farm is a location hosting multiple computers all connecting to the internet through the same network, wherein individuals at the laptop farm assist remote individuals with logging on to the computers. This practice makes it appear that the remote individual is physically located at the location of the laptop farm, as the IP address for the laptop will be that of the laptop farm. Based on my training and experience, U.S. companies sometimes monitor the IP addresses of remote IT workers; a company would find it suspicious

if an IT worker claiming to be located in the United States used a foreign IP address.

27. A review of messages in Subject Account-3 shows that DIDENKO is operating "laptop farms" in the United States. The messages show that, when DIDENKO's customers request an account associated with a U.S. identity and are then employed by a U.S. company, DIDENKO provides them a location in the United States that will host the company-provided computer for a fee. To accomplish this, DIDENKO works with U.S.-based co-conspirators who receive computers, set up the computers, and maintain the computers' internet connection. The participation of these co-conspirators is essential to the scheme to deceive U.S. companies hiring remote IT workers because the U.S. companies typically only ship a computer for the IT worker's use to a U.S. address when the IT worker claims to be located in the United States. On behalf of his customers, DIDENKO facilitated the shipment of remote IT worker computers to multiple U.S. locations:

28. **2353 Upper Greens Place, Virginia Beach, VA 23456 ("U.S. Address-1")** –A review of messages from Subject Account-3 shows that in September 2023, DIDENKO had an exchange with an unidentified customer ("Customer-2") in which Customer-2 asked for help in receiving a computer in the United States. DIDENKO replied by providing U.S. Address-1 and the name [redacted] (U.S. Co-Conspirator-1). Approximately three days later, Customer-2 sent DIDENKO a message containing a tracking number for a package being sent to U.S. Co-Conspirator-1 at U.S. Address-1. Approximately two days later, DIDENKO sent Customer-2 a message, "Hi! Your USA PC is activated." "We can provide anydesk[3] access."

[3] Based on my training and experience, and review of AnyDesk's website, AnyDesk is an application that allows users to log onto another laptop remotely through the AnyDesk application.

"200$ is prepayment".

29. Virginia driver's license records for U.S. Co-Conspirator-1 list U.S. Address-1 as the residence address. Based on records of the DHS, U.S. Co-Conspirator-1 is a Ukrainian national who previously had a J1 visa and departed the United States in September 2016. In June 2022, U.S. Co-Conspirator-1 was lawfully admitted to the United States.

30. As previously described, Subject Account-2 included a spreadsheet of proxy identities; the spreadsheet lists U.S. Co-Conspirator-1's name as being associated with an Overseas Platform-1 account and a U.S. MST-2 account. Subject Account-2 contained an image of U.S. Co-Conspirator-1's passport, which according to U.S. MST-2's records was used to verify her account at U.S. MST-2.

31. According to records of U.S. MST-1, between February and December 2023, DIDENKO's U.S. MST-1 account remitted 16 payments to U.S. Co-Conspirator-1's U.S. MST-1 account totaling $2,030.53. Of the 16 payments, 13 were $100 payments.

32. **821 W. King St, Jefferson City, TN 37760 ("U.S. Address-2")** – A review of emails found in Subject-Account 2 shows that, in November 2023, DIDENKO was forwarded an email containing confirmation of a laptop shipment that arrived at U.S. Address-2 under the name of [redacted] ("U.S. Co-Conspirator-2"). Records of U.S. MST-1 show that on or about December 2, 2023, DIDENKO sent U.S. Co-Conspirator-2 $130. Records of U.S. MST-1 list U.S. Address-2 as an active address for U.S. Co-Conspirator-2's account.

33. A review of Online Message Provider-1 messages found in Subject Account-3 shows that, in October 2023, DIDENKO received via chat an inquiry from Customer-2 if he/she could have another computer sent to U.S. Co-Conspirator-1's address. DIDENKO responded, "Ofc you can, but let's use another address" and then provided U.S. Address-2 and the name

[redacted] ("U.S. Co-Conspirator-3"). Approximately five days later, Customer-2 messaged DIDENKO with a tracking number for the shipment. The following day, DIDENKO messaged a confirmation that the laptop had been picked up.

34. Tennessee driver's license records for U.S. Co-Conspirator-3 list a residence address in the same city as U.S. Address-2. Based on U.S. Department of State visa records , U.S. Co-Conspirator-3 is a Ukrainian national with an F1 visa.

35. According to records of U.S. MST-1, on October 20, 2023, and October 31, 2023, DIDENKO's U.S. MST-1 account remitted payments of $8 and $50, respectively, to U.S. Co-Conspirator-3's U.S. MST-1 account.

36. **3067 5th Avenue Apt 202, San Diego, CA 92103 ("U.S. Address-3")** – A review of messages found in Subject Account-3 shows that, in November 2023, DIDENKO had an exchange with an unidentified customer ("Customer-3") in which Customer-3 wrote, "Hi, I need remote PC connection in US. Company will send PC in US." After DIDENKO responded, "We can help you". Customer-3 asked, "Which state and price?" DIDENKO answered, "[I]n california 400". Customer-3 asked, "[H]ow many PCs is he managing now". DIDENKO answered, "15 now". Later in the conversation, DIDENKO sent a message to Customer-3 with U.S. Address-3 and the name [redacted] ("U.S. Co-Conspirator-4"). Approximately two weeks later, Customer-3 messaged DIDENKO a shipping tracking number for a laptop shipment. Approximately two days later, DIDENKO messaged in reply, "The agent informed me 2 minutes ago that we received the package."

37. Based on records of DHS, U.S. Co-Conspirator-4 is a Ukrainian national who arrived in the United States in June 2022 and was lawfully admitted to the United States.

Other Co-Conspirators

38. A review of Online Message Provider-1 messages found in Subject Account-3 shows that often when DIDENKO communicates with customers who have problems logging into computers remotely, DIDENKO refers them to "Simon", the Technical Manager.

a. For example, in September 2023, Customer-2 asked DIDENKO via chat to "please check the internet connect". DIDENKO told Customer-2 to "please, ping simon". After Customer-2 asked, "who is simon", DIDENKO responded: "Technical Manager (He will help if your computer is offline or there are problems with the Internet)" and then provided an Online Message Provider-1 id and a Telegram handle for "Simon".

39. A review of Online Message Provider-1 messages found in Subject Account-3 shows that if there are chat discussions about paying rent for access to U.S. MST-2 accounts, DIDENKO sometimes refers customers to "Denys", the Finance Manager.

a. For example, in December 2022, DIDENKO messaged Customer-2 via Online Message Provider-1 chat, "The payment date is fixed on the 13th of each month." "I am glad to introduce you to my financial manager Denys. From that moment, he will remind you about rent payments." "Please add it to your contacts. He has either already sent you an inquiry or will do it very soon." DIDENKO then provided an Online Message Provider-1 id and Telegram handle for "Denys".

40. DIDENKO uses Trello to further the scheme. Trello is an online work management tool which allows businesses and individuals to draft plans, collaborate on projects, organize operations and track progress of assigned tasks. Records obtained based on a search warrant of DIDENKO's email accounts revealed that DIDENKO had an account with Trello. Records obtained from a search warrant of this Trello account include screenshots of

conversations that took place on other messaging platforms where users discuss payments and account suspensions. There are also screenshots of registrations for U.S. MST-2 accounts.

B. Examples of The Scheme

41. In an effort to succinctly illustrate DIDENKO's criminal conduct, this affidavit provides examples of DIDENKO's interactions to sell or rent accounts, the design of his infrastructure to support this scheme, the documentation kept to organize the scheme, and payment methods. A review of evidence gathered in the investigation shows that the goal of this scheme is to profit by providing remote IT workers with proxy accounts and proxy internet access in order for the IT workers to fraudulently gain employment and transfer employment income to foreign bank accounts.

42. A review of Online Message Provider-1 messages between DIDENKO and an unidentified customer ("Customer-4") found in Subject Account-3 demonstrates the way the scheme was effected by DIDENKO:

Creation of a Proxy U.S. Platform-1 Account

a. On or about May 31, 2023, Customer-4 requested to rent a U.S. Platform-1 account. DIDENKO responded, "we can help" "We recommend only Ukraine now. it's more safety". Customer-4 asked, "How much is it?" DIDENKO replied, "80$ is prepayment, 80$ per/m". DIDENKO provided options to pay him in USDT (Tether stablecoin cryptocurrency), BUSD (Binance stablecoin cryptocurrency), USDC (USD Coin stablecoin cryptocurrency), and via U.S. MST-2. After some additional discussion, Customer-4 wrote: "i will pay now". DIDENKO wrote: "Your order is accepted. I think you will get it tomorrow."

b. On or about June 1, 2023, DIDENKO sent to Customer-4 remote computer login

information, and email and U.S. Platform-1 login information for an account under the name "Ruslan Bairamov." The same email and password appears in aforementioned spreadsheet of proxy identities located in Subject Account-2.

Creation of a Proxy U.S. Platform-1 Account with a Stolen U.S. Identity

c. In three instances, Customer-4 requested via Online Message Provider-1 chat that DIDENKO create U.S. MST-2 accounts with the name of an identified U.S. Person ("U.S. Person-1"). According to State Department records for a June 2021 application for a U.S. passport, U.S. Person-1 is a U.S. citizen born in Texas.

d. First, on or about June 2, 2023, Customer-4 wrote, "I hope to buy [U.S. MST-2] account with my name. [U.S. Person-1]"

i. Customer-4 stated, "I got a job offer with [U.S. Person-1]. They need bank account with [U.S. Person-1] name." DIDENKO responded, "We can create [U.S. MST-2] account with your name. But we do not recommend it for use. It is not safe and we are not responsible for such an account. We have a lot of experience and recommend using accounts of real people. We have such accounts and we can sell or rent them. But in any case, if you need an account with your name, we can create it for you." Customer-4 replied, "I need bank account with same name. If not company does not accept it. I am going to use virtual bank in the [U.S. MST-2] account." After Customer-4 asked DIDENKO how much it would cost, DIDENKO wrote, "250$. Within 72h after prepayment." After additional discussion, DIDENKO wrote, "we will provide this acc asap" "and passport too". Customer-4 added, "i already bought driver licnese [sic] for 80 USD" "and SSN with 30

USD". Customer-4 sent DIDENKO a birthdate, a Texas address, and a photo, "if you need details for passport use these". In response to the photo, DIDENKO wrote, "No need" "the quality is not good. it will be clear that this is a fake passport."

ii. On or about June 6, 2023, DIDENKO sent Customer-4 U.S. MST-2 login information, which included email address, [redacted]@gmail.com. This email appears in DIDENKO's spreadsheet of proxy identities next to the name of U.S. Person-1.

iii. According to records of U.S. MST-2, on or about June 2, 2023, an account was registered with U.S. Person-1's name, email address [redacted]@gmail.com, and a Ukrainian passport.

e. Second, in August 2023, Customer-4 asked for another account.

i. On or about August 28, 2022, Customer-4 messaged DIDENKO "Just make [U.S. Person-1] [U.S. MST-2]." "But please make another passport for it. Do not use the previous passport you used for old [U.S. Person-1] [U.S. MST-2]." DIDENKO responded with methods to pay him and quoted a price of "250$".

ii. On or about September 5, 2023, DIDENKO sent to Customer-4 U.S. MST-2 login information, which included email address: [redacted]@gmail.com. This email appears in DIDENKO's spreadsheet of proxy identities next to the name of U.S. Person-1.

iii. Records of U.S. MST-2 show that an account was registered on or about August 30, 2023, with U.S. Person-1's name, email address

[redacted]@gmail.com, and a Ukrainian passport.

iv. The Ukrainian passports for the [redacted]@gmail.com and [redacted]@gmail.com U.S. MST-2 accounts had different photos but identical signatures. Based on my training and experience, this pattern is an indication that the passports were forgeries.

f. Third, in October 2023, Customer-4 requested a third account.

i. On or about October 27, 2023, Customer-4 wrote to DIDENKO, "I request one more [U.S. MST-2] with [U.S. Person-1]".

ii. On or about October 30, 2023, DIDENKO sent to Customer-4 U.S. MST-2 login information, which included email address: [redacted]@gmail.com. This email appears in DIDENKO's spreadsheet of proxy identities next to the name of U.S. Person-1.

iii. Records of U.S. MST-2 show that an account was registered on or about October 28, 2023, with U.S. Person-1's name, email address [redacted]@gmail.com, and a Ukrainian passport.

Providing Remote Access to U.S.-Based Computers

g. On or about June 7, 2023, Customer-4 told DIDENKO via Online Message Provider-1 message, "I have got a job from US company. They are going to deliver computer this week. Can you help me with this? And he must be in Texas." Based on my training and experience, U.S. companies sometimes mail a computer to a remote IT worker for use in completing a work contract.

h. On or about June 7, 2023, DIDENKO responded, "We can receive laptop in another state" and proceeded to provide an address for a commercial shipping

service's "access point", i.e., a package pick-up/delivery location, in Virginia. DIDENKO quoted the fee as, "200$ is prepayment (when we get the laptop and you get access)" "200$ per/m". Customer-4 asked, "So when the company does shipping which receiver name do they have to write on it?" DIDENKO responded, "you can tell them to send parcel to your wife's name: [U.S. Co-Conspirator-1]". Customer-4 clarified that the company "will ship with [U.S. Person-1] name" "and a family member can receive it" "I introduced them [U.S. Co-Conspirator-1] is my wife". Approximately three weeks later, DIDENKO provided Customer-4 with remote log-in credentials for the computer.

i. On or about August 18, 2023, Customer-4 sent U.S. Address-1 to DIDENKO and asked, "Does this address work for laptop delivery?" "I provided this address." DIDENKO responded, "yes, sure".

j. On or about October 2, 2023, DIDENKO messaged Customer-4, "Hi! Friend, we have changed US address. Let me know when you need a new one". DIDENKO provided US Address-2 followed by, "New address to new PC's. You can use anyname".

C. <u>Financial Transactions</u>

43. DIDENKO utilizes his U.S. MST-2 account to receive payments he earns from his scheme.

a. For example, according to records of Subject Account-3, on or about September 24, 2019, an unidentified customer ("Customer-5") messaged DIDENKO asking him to create a U.S. Platform-1 account. DIDENKO advised Customer-5 of the $170 prepayment amount, which included purchase of a computer, modem, and

passport data. Customer-5 asked DIDENKO, "how should I pay for that prepayment?" DIDENKO responded "[U.S. MST-2]". Customer-5 subsequently replied, "let me know your account email." "I will send now". DIDENKO then shared his email address, Subject Account-2, which is directly linked to his U.S. MST-2 account.

b. Records of U.S. MST-2 show that, on or about September 24, 2019, DIDENKO's account received $170 from a U.S. MST-2 account based in China. Records of U.S. MST-2 also show that at least two additional U.S. MST-2 accounts were utilized to remit payments to DIDENKO for his services from Customer-5. These accounts were also based in China. In total, between approximately July 2019 and approximately April 2022, records of U.S. MST-2 show that DIDENKO's account received 148 payments totaling $23,773 between these known China-based accounts.

44. DIDENKO also utilizes his U.S. MST-2 account to receive funds for his "credit card" services portion of his scheme.

a. For example, according to records of Subject Account-3, on or about September 28, 2019, Customer-5 inquired about his U.S. Platform-1 account by asking, "1. before passing the [U.S. Platform-1] verification, shouldn't I make profile completion percent 100%? 2. may I setup payment method? 3. as you know, the initial connects is only 20. can you charge $50 into the account, I will send payment for that?" DIDENKO responded, "no. it will be better if we make this payment by credit card", "you can send me funds and I will replenish the card". Customer-5 then replied, "I will send $100 now", "what is your [U.S. MST-2]

account?", [redacted]@gmail.com?" To which DIDENKO responded "ok".

b. Records of U.S. MST-2 show that, on September 28, 2019, $100 was remitted from a China-based U.S. MST-2 account to DIDENKO's. On the same day, DIDENKO's U.S. MST-2 account transferred $100 to DIDENKO's linked Ukraine-based bank account affiliated with a payment card, "414949XXXXXX1010".

45. According to records of U.S. MST-2, DIDENKO utilizes multiple accounts to layer funds for his scheme. DIDENKO withdraws the funds held in his U.S. MST-2 account to the bank accounts based in Ukraine. DIDENKO had at least ten Ukraine-based bank accounts linked to his U.S. MST-2 account. Of these, four accounts were held under his name. Between in or about December 2018 and June 2022, DIDENKO withdrew a total of $202,422.83 from his U.S. MST-2 account to Ukraine-based bank accounts, including as follows.

a. On March 3, 2021, a Ukraine-based U.S. MST-2 account ("Account-1") transferred $150 to DIDENKO's account. On the same day, DIDENKO's U.S. MST-2 account transferred $150 to a Russia-based account ("Account-2").

b. On April 16, 2021, Account-1 transferred $1,425 to DIDENKO's account. On the same day, DIDENKO's account transferred $1,425 to Account-2.

c. On September 27, 2021, a United Kingdom-based U.S. MST-2 account ("Account-3") transferred $1,876 to DIDENKO's account. On the same day, DIDENKO's account transferred $1,876 to a Bosnia and Herzegovina-based U.S. MST-2 account ("Account-4").

d. Also on September 27, 2021, Account-3 transferred $1,992 to DIDENKO's account. On the same day, DIDENKO's account transferred $1,992 to Account-

4.

46. A review of messages found in Subject Account-3 shows that DIDENKO and his customers were aware the accounts are subject to scrutiny by U.S. authorities and/or U.S. MSTs.

a. For example, on September 6, 2022, DIDENKO's customer ("Customer-6") messaged DIDENKO asking, "can you exchange $2000 now?" "[U.S. MST-1] to [U.S. MST-2]" "same [U.S. MST-1]?" To which DIDENKO responded, "We can". Customer-6 then shared a screenshot of a payment confirmation of $2,000 to Oleksandr Didenko. When Customer-6 asked, "Is it holding now?" To which DIDENKO responded, "we do not recommend sending large amounts together. If would be better to break it up into smaller amounts. Now you need to wait for the transaction to be completed . . . ."

b. On September 6, 2022, a payment of $2,000 was initiated to be sent to DIDENKO's account and was finalized on September 8, 2022.

c. On May 12, 2023, DIDENKO's customer ("Customer-4") messaged DIDENKO asking, "Is it safe if I buy real person's [U.S. MST-2] more than fake name?" To which DIDENKO responded, "of course".

d. On or about October 25, 2023, Customer-4 messaged DIDENKO asking, "The same payroll day I will get payment about 12k from two companies." "Is it safe then?" DIDENKO later responded, "if you able – better use another one [U.S. MST-2] acc for that".

e. Based on my training and experience, DIDENKO and his customers were discussing a potential risk of account review and/or account closure by U.S. MST-2 due to suspicious financial activities in connection to the scheme.

D. Use of Stolen U.S. Person Identities

47. DIDENKO's scheme involves U.S. persons who are victims of identity theft or have loaned their identity out for use by others. A search of Subject-Account-2 revealed pictures of a several U.S. identification documents such as passports and driver's licenses. According to U.S. Department of State passport information, six of the U.S. passports found in DIDENKO's account were reported as either lost or stolen.

U.S. Person-1

48. As stated, DIDENKO's Online Message Provider-1 chats with Customer-4 show that Customer-4 was using the identity of U.S. Person-1, a U.S. citizen born in Texas. U.S. Person-1's information was found on DIDENKO's spreadsheet of proxy identities.

49. According to business records of U.S. Company-1, in August 2023, an identified U.S. Company ("U.S. Company-5") offered an employment contract to an individual posing as U.S. Person-1, who was using the email address [redacted]@gmail.com. U.S. Company-5 subsequently made payments to the U.S. MST-2 account for this U.S. Person-1 identity. The person posing as U.S. Person-1 provided U.S. Company-5 a signed I-9 Employment Eligibility Verification form and a signed IRS W-4 Employee's Withholding Certificate form. The employment records also included a Social Security card and a Texas driver's license for U.S. Person-1. The driver's license had a photo of an Asian male (which did not match the photo in the Ukrainian passport (a white male) used to create the U.S. MST-2 account in the name of U.S. Person-1). State driver's license records revealed that the real U.S. Person-1 is a black male with a Texas address.

50. Additionally, on or about April 25, 2024, your affiant interviewed a human resources (HR) representative for U.S. Company-6, a technology staffing company in Maryland.

The HR representative noted that an IT worker using the identity U.S. Person-1 was hired on November 13, 2023, to work on a contract with a government agency. To verify employment eligibility, the IT worker posing as U.S. Person-1 provided a Texas driver's license with a picture of an Asian male, the same ID provided to U.S. Company-5. The HR representative also stated that the IT worker posing as U.S. Person-1 was on "disability leave" and needed to be fingerprinted for the contract with the government agency. Based on my training and experience, I know that IT workers perpetrating these schemes often tell employers that they have various calamities befall them or personal issues when they are required to do something for the employer that necessitates in-person contact. Based on records from E-Verify, on or about November 13, 2023, U.S. Company-6 submitted U.S. Person-1's identity documents to the E-Verify system and listed the email address associated with U.S. Person-1 as [redacted]@gmail.com."

51. Additionally, based on records from E-Verify, on or about July 18, 2023, U.S. Company-7, a staffing company in Pennsylvania, submitted all the same information for employment of U.S. Person-1, to include the same email address. E-Verify records further show that, in March 2020, a Texas-based refinery submitted to E-Verify information about U.S. Person-1, with a different email address. Analysis of these records, to include the pre-pandemic employment in a different industry in U.S. Person-1's home state, thus, shows there is probable cause to believe that U.S. Person-1's identity was fraudulently submitted to both U.S. Company-6 and U.S. Company-7.

U.S. Person-2

52. Investigators interviewed U.S. Person-2, who is a U.S. citizen born in Pennsylvania. U.S. Person-2 stated that his/her identity had been stolen and that they had

received various indications of the same, including a laptop from an identified U.S. Company ("U.S. Company-1") at his/her actual residence despite that U.S. Person-2 did not work for that company.

53. According to business records of four U.S. companies, U.S. Person-2's identity was used to gain employment with multiple identified U.S.-based companies. U.S. Person-2's name, address, and Social Security Number were used to apply to four identified U.S. companies.

a. Based on business records and an interview, in early January 2024, an unidentified male posing as U.S. Person-2 applied to an identified U.S. company ("U.S. Company-2"), specifically for a contract position with the U.S. government agency.

i. An employee of U.S. Company-2 conducted an interview with the individual claiming to be U.S. Person-2 and noticed the individual was an Asian male who spoke broken English. U.S. Person-2 is a white male. The individual requested a laptop be sent to U.S. Address-2, which is not U.S. Person-2's actual residence.

ii. According to U.S. Company-2's records, the company conducted a check for employment eligibility of U.S. Person-2 with DHS's E-Verify system, using the identity documents provided by the individual. The individual impersonating U.S. Person-2 provided a Pennsylvania driver's license with U.S. Person-2's name, date of birth, and address, but a different license number than that of the real U.S. Person-2's license.

b. Based on interviews, in or about March 2024, an unidentified individual posing as U.S. Person-2 had received a job offer at another identified U.S. company ("U.S. Company-3").

i. U.S. Company-3 conducted three video interviews of the individual who indicated he was based in Pennsylvania and was willing to relocate. U.S. Company-3 used a third-party to initiate the individual's background check, which he passed. U.S. Company-3 sent a prepaid debit card containing a relocation bonus as well as a laptop to the individual's requested address, U.S. Address-2. The individual initially requested for the relocation bonus to be deposited directly into his account, but eventually agreed for the prepaid debit card to be sent to the U.S. Address-2 per the policy of U.S. Company-3.

ii. Upon notification by U.S. Person-2 to U.S. Company-3 that the unidentified individual fraudulently used U.S. Person-2's identity to apply for the position, U.S. Company-3 terminated the unidentified individual's employment. The prepaid debit card funds had been already used for on-line purchases, rather than relocation expenses.

c. Based on an interview, in February 2024, an unidentified individual applied for employment at an identified U.S. company ("U.S. Company-4").

i. The unidentified individual used U.S. Person-2's name, a doctored license, and a counterfeit Social Security card, and provided a Tennessee residential address. U.S. Company-4 conducted I-9 verification of these documents, which were identified as false documents.

54. U.S. Person-2's name appears in DIDENKO's spreadsheet of proxy identities where two accounts associated with his name are marked as "Sold". In December 2023, DIDENKO exchanged Online Message Provider-1 messages with Customer-4 in which Customer-4 requested DIDENKO create a U.S. MST-2 account in U.S. Person-2's name. In January 2024, Customer-4 asked, "Is Tenneessee [sic] delivery office working now?" "New laptop will be delivered soon" "Delivery name will be [U.S. Person-2]".

55. Additionally, records of E-Verify show that four additional U.S. Companies (U.S. Company-8, -9, -10, -11), all submitted employment eligibility queries for workers posing as U.S. Person-2 between January 4, 2024, and March 11, 2024, with false documentation.

U.S. Person-3

56. On or about September 22, 2023, DIDENKO exchanged Online Message Provider-1 messages on Subject Account 3 with an unidentified customer ("Customer-7"). Customer-7 informed DIDENKO, "I have shipped one equipment to VA address." A review of the Online Message Provider-1 conversation shows that this laptop was associated with an IT worker using the identity of U.S. Person-3, and was issued by U.S. Company-12, a staffing company.

57. Business records of U.S. Company-13, a luxury retail chain, show that it contracted the IT worker posing as U.S. Person-3 for IT work between October 2, 2023, until November 17, 2023, through U.S. Company-12. A review of New York driver's license data and U.S. Department of State records shows that U.S. Person-3 is a U.S. citizen residing in New York.

E. False Information Transmitted to the U.S. Government

58. On or about the dates listed below, the remote IT workers who were customers

of DIDENKO applied for employment with U.S. companies and caused the U.S. companies to transmit false information, to include false information about U.S. persons' identities and false documents to USCIS via the E-Verify system, in order to verify employment eligibility:

Sub-¶	U.S. Person Identity	Date	Document 1	State	Document 2	Employer
a.	U.S. Person-1	7/19/2023	State Driver's License/ID	TX	Social Security (SS) Card	U.S. Company-7
b.	U.S. Person-1	11/13/2023	State Driver's License/ID	TX	SS Card	U.S. Company-6
c.	U.S. Person-2	1/2/2024	State Driver's License/ID	PA	SS Card	U.S. Company-2
d.	U.S. Person-2	1/9/2024	State Driver's License/ID	PA	SS Card	U.S. Company-8
e.	U.S. Person-2	2/21/2024	State Driver's License/ID	PA	SS Card	U.S. Company-4
f.	U.S. Person-2	2/22/2024	State Driver's License/ID	PA	SS Card	U.S. Company-9
g.	U.S. Person-2	3/6/2024	State Driver's License/ID	PA	SS Card	U.S. Company-10
h.	U.S. Person-2	3/13/2024	State Driver's License/ID	PA	Birth Certificate	U.S. Company-11
i.	U.S. Person-3	9/20/2023	State Driver's License/ID	NY	SS Card	U.S. Company-12

59. Further, the scheme has caused false information to be transmitted to IRS and SSA. Based on my training and experience, I know that U.S. companies are required to annually report wages and earnings to IRS and SSA for all their employees. As previously explained, U.S. Person-1's, U.S. Person-2's, and U.S. Person-3's identities were successfully used to gain employment and earn wages with at least 5 companies (U.S. Company-2, -3, -4, -6. -12). Moreover, a review of email records for Subject Account-2 showed that at least 13 U.S. identities may have been compromised as part of the scheme. Thus, based on the foregoing, there is probable cause to believe that U.S. persons have had wages falsely reported to IRS and SSA as

part of the scheme.

F. Connection to North Korea

Background on North Korea IT Worker Schemes

60. According to a May 2022 public advisory by the Department of State, the Department of the Treasury, and the Federal Bureau of Investigation, North Korea has dispatched thousands of highly skilled IT workers around the world, earning revenue that contributes to the North Korean weapons programs, in violation of U.S. and UN sanctions. These workers (i) surreptitiously obtain IT development employment from companies around the world; (ii) misrepresent themselves as foreign (non-North Korean) or U.S.-based teleworkers, including by using VPNs, virtual private servers ("VPSs"), third-country internet protocol ("IP") addresses, proxy accounts, and falsified or stolen identification documents; (iii) develop applications and software spanning a range of sectors and industries; and (iv) use privileged access gained through employment for illicit purposes, including enabling malicious cyber intrusions by other DPRK actors. These IT workers are subordinate to North Korea's Munitions Industry Department ("MID"). MID is involved in key aspects of North Korea's missile program, including overseeing the development of North Korea's ballistic missiles, weapons production, and research and development programs.

Connection to a North Korea IT Worker Cell

61. As previously stated, on or about September 22, 2023, DIDENKO exchanged Online Message Provider-1 messages on Subject Account 3 with Customer-7 about a computer that had been shipped to the Virginia laptop farm. On or about September 29, 2023, Customer-7 followed up, "This is the first time to deliver laptop to you. I will see this first experience and decide if my team can continue or not." DIDENKO responded, "Please don't worry. We received

these packages. I'll let you know when we get it online." By October 3, 2023, the laptop had still not been set up at the Virginia address, and Customer-7 wrote, "Can you deliver laptop back today? I can not trust your delivery address any more." DIDENKO replied, "Let me know address, please. I will do everything possible." Customer-7 responded that if it was not possible to set up the laptop that day, "then deliver it to following address as THE FASTEST option and share TRACKING INFO. [redacted], Litchfield Park, AZ 85340". In reference to this address, DIDENKO inquired, "Let me know name of receiver also". Customer-7 replied, "Christina Chapman". On or about October 6, 2023, Customer-7 confirmed to DIDENKO, "I've received laptop and set it up."

62. Based on information provided to me from a separate investigation, Christina Chapman is a U.S. person living in Arizona who has been operating a laptop farm in her home. On or about October 27, 2023, the FBI conducted a court-authorized search warrant of Chapman's residence and discovered more than 90 computers being run through remote connections. Attached to the computers were notes affiliating each computer with a U.S. company and with a U.S. identity, which through additional queries of the U.S. company records and E-Verify data at DHS, have been determined to be used by remote (non-U.S.) IT workers using the U.S. identities.

63. Additionally, three U.S. person identities that were associated with computers found in Chapman's residence have separately been connected to a North Korean IT worker scheme through an investigation by and business records of a U.S. Cyber Security Firm, as follows.

a. On September 6, 2023, a U.S. Cyber Security firm received a tip that an IP address associated with a state-sponsored espionage group tied to North Korea, was used

to update the LinkedIn page of U.S. Person-4, a former contractor engaged by the U.S. Cyber Security firm between September 21, 2022 and March 3, 2023. The U.S. Cyber Security firm immediately assembled an incident response team to investigate which led to the discovery that U.S. Person-4 used a number of tactics, techniques and procedures ("TTPs") associated with the identified North Korean group, including remote control web browser extensions to provide remote access to the U.S. Cyber Security firm's system via proxy services and VPNs to mask his IP address. The U.S. Cyber Security firm expanded its review to determine if any similar TTPs were used by any current and former contractors or employees and identified eight additional, former contractors who had exhibited similar TTPs. All nine of the former contractors were engaged to perform work at the U.S. Cyber Security firm through third-party staffing agencies and were not directly employed or paid by the U.S. Cyber Security firm. Among the eight additional DPRK linked employees were two additional remote IT workers related to Chapman. These individuals were U.S. Person-5 and U.S. Person-6.

b. Separately, in or about November 2023, a U.S. Cyber Security firm discovered documents in an online storage platform related to North Korean IT workers' attempts to obtain employment as remote workers. The Cyber Security firm assessed with "high confidence" that these documents can be attributed to the same espionage group tied to North Korea. The Cyber Security firm stated, "Several of the documents we discovered contained information that more definitively points to North Korea. Many of the passwords associated with these documents were made through Korean language typed on a U.S. keyboard, and

some passwords include words only used in North Korea. Furthermore, Korean keyboard language settings were found on computers used by threat actors behind these campaigns." The documents included guides and tips related to topics about securing employment, writing a cover letter, building a resume, sample resumes of purported IT workers, and scripts for interviews. Several documents were related to online job postings seeking employees that the North Korean IT workers captured, including three jobs with U.S. employers that were later tied through business records to the computers found in Chapman's residence during the execution of the search warrant.

Didenko's Acknowledgment of Work with North Korean IT Workers

64. Online Message Provider-1 messages found in Subject Account-3 show that DIDENKO had been communicating with an unidentified customer ("Customer-8") since October 2021. On or about March 10, 2023, DIDENKO asked Customer-8, "[A]re all your programmers in China? Are there programmers who are in North Korea? [L]ast year I received information that some of my clients are from North Korea, I was very surprised, I thought it was impossible". Customer-8 answered, "I don't know .. but we are all in China" "who said like that?" DIDENKO responded, "[O]ne of our clients". Customer-8 then asked, "[C]an I have his Online Message Provider-1 id? I am interested in such things".

65. On or about March 25, 2024, an individual purporting to be "Oleksandr Didenko", with contact information of Subject Account 2 and Subject Phone Number 1, sent an electronic message to a tip line stating, "This is about North Korean programmers. . . . I work alongside people who are willing to sell their accounts for a small amount of money, and North Korean IT specialists are willing to pay a lot of money for it (I think they are from North Korea,

but I'm not 100% sure. I have their contacts)."

G. Conclusion

66. Based on the foregoing, your affiant submits that there is probable cause to believe that, from approximately January 2018 until the present, DIDENKO and others known and unknown, have violated, caused to be violated, aided and abetted a violation, or conspired to violate the following statutes:

a. DIDENKO and the remote IT workers caused false information to be transmitted to U.S. government agencies located in the District of Columbia, to include the Department of Homeland Security, the Internal Revenue Service, and the Social Security Administration, thereby defrauding the United States by interfering with and obstructing a lawful government function of these agencies by means of deceit, craft, trickery, and dishonesty, in violation of 18 U.S.C. § 371.

b. DIDENKO and the remote IT workers devised a scheme or artifice to defraud companies, or obtain money or property by means of false or fraudulent pretenses from such companies, i.e., the employment of individuals using false identities, and transmitted by means of interstate and foreign wires, specifically, through U.S. Platform-1, U.S. Platform-2, U.S. MST-1, U.S. MST-2, the purpose of executing such scheme or artifice, in violation of 18 U.S.C. §§ 1343 & 1349 (wire fraud and conspiracy).

c. The remote IT workers, with assistance from DIDENKO, knowingly transferred, possessed, or used, without lawful authority, a means of identification of another person, while committing wire fraud, in violation of 18 U.S.C. § 1028A.

d. The remote IT workers, with assistance from DIDENKO, knowingly possessed identification documents or a false identification document with the intent such document or feature be used to defraud the United States, i.e., in the transmitting of those documents to the Department of Homeland Security, in violation of 18 U.S.C. §§ 1028(a)(7), (b)(1)(D), (c)(3)(A) & (f).

e. The remote IT workers, while located outside the United States and while operating under a false identity and through the submission of false information, performed work for U.S. companies through the use of computers located at U.S. laptop farms, and with the assistance and aid of DIDENKO. The overseas workers were, in fact, aliens to the United States and the overseas workers' employment in the United States through the scheme and the assistance and aid of DIDENKO, who was paid for his services, violated 8 U.S.C. § 1324a and 18 U.S.C. §§ 2, 371.

f. DIDENKO and the remote IT workers knowingly conducted financial transactions with the proceeds of the aforementioned criminal activity, to include transfers between DIDENKO's accounts and to the accounts of the others involved in the scheme, in violation of 18 U.S.C. §§ 1956(a)(1)(B)(i) & (h) (a)(2)(A), & (h).

g. DIDENKO, through Upworksell.com, marketed and sold financial accounts with U.S.-based MSTs for use in the United States, and which the remote IT workers provided to U.S.-based employers as a means of violation, thus causing the transportation and transmission of funds that were from a criminal offense or are intended to be used to promote unlawful activity, all without being registered as a money transmitting service with state or federal authorities, in violation of 18 U.S.C. § 1960.

REQUEST TO SUBMIT WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

67. I respectfully request, pursuant to Rules 4.1 and 41(d)(3) of the Federal Rules of Criminal Procedure, permission to communicate information to the Court by telephone in connection with this Application for an Arrest Warrant. I submit that Assistant United States Attorney Karen P. Seifert, attorney for the United States, is capable of identifying my voice and telephone number for the Court.

CONCLUSION

68. Based on the forgoing, I request that the Court issue the proposed arrest warrant.

Respectfully submitted,

David Booth
Special Agent
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on April 29, 2024.

HONORABLE MOXILA A. UPADHYAYA
UNITED STATES MAGISTRATE JUDGE

May 16, 2022

GUIDANCE ON THE DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA INFORMATION TECHNOLOGY WORKERS

The U.S. Department of State, the U.S. Department of the Treasury, and the Federal Bureau of Investigation (FBI) are issuing this advisory for the international community, the private sector, and the public to warn of attempts by Democratic People's Republic of Korea (DPRK, a.k.a. North Korea) information technology (IT) workers to obtain employment while posing as non-North Korean nationals. There are reputational risks and the potential for legal consequences, including sanctions designation under U.S. and United Nations (UN) authorities, for individuals and entities engaged in or supporting DPRK IT worker-related activity and processing related financial transactions.

The DPRK dispatches thousands of highly skilled IT workers around the world to generate revenue that contributes to its weapons of mass destruction (WMD) and ballistic missile programs, in violation of U.S. and UN sanctions. These IT workers take advantage of existing demands for specific IT skills, such as software and mobile application development, to obtain freelance employment contracts from clients around the world, including in North America, Europe, and East Asia. In many cases, DPRK IT workers represent themselves as U.S.-based and/or non-North Korean teleworkers. The workers may further obfuscate their identities and/or location by sub-contracting work to non-North Koreans. Although DPRK IT workers normally engage in IT work distinct from malicious cyber activity, they have used the privileged access gained as contractors to enable the DPRK's malicious cyber intrusions. Additionally, there are likely instances where workers are subjected to forced labor.

This advisory provides detailed information on how DPRK IT workers operate; red flag indicators for companies hiring freelance developers and for freelance and payment platforms to identify DPRK IT workers; and general mitigation measures for companies to better protect against inadvertently hiring or facilitating the operations of DPRK IT workers. An Annex provides additional information on DPRK IT workers from reports produced by the UN 1718 Sanctions Committee's DPRK Panel of Experts. The FBI encourages U.S. companies to report suspicious activities, including any suspected DPRK IT worker activities, to local field offices.

DPRK IT WORKERS: BACKGROUND

DPRK IT workers provide a critical stream of revenue that helps fund the DPRK regime's highest economic and security priorities, such as its weapons development program. DPRK leader Kim Jong Un recognizes the importance of IT workers as a significant source of foreign currency and revenue and supports their operations.

There are thousands of DPRK IT workers both dispatched overseas and located within the DPRK, generating revenue that is remitted back to the North Korean government. DPRK IT workers are located primarily in the People's Republic of China (PRC) and Russia, with a smaller number in Africa and Southeast Asia. These IT workers often rely on their overseas contacts to obtain freelance jobs for them and to interface more directly with customers.

All DPRK IT workers earn money to support North Korean leader Kim Jong Un's regime. The vast majority of them are subordinate to and working on behalf of entities directly involved in the DPRK's UN-prohibited WMD and ballistic missile programs, as well as its advanced conventional weapons development and trade sectors. This results in revenue generated by these DPRK IT workers being used by the DPRK to develop its WMD and ballistic programs, in violation of U.S. and UN sanctions. Many of these entities have been designated for sanctions by the UN and United States. DPRK entities dispatching DPRK IT workers include:

- **The 313 General Bureau of the Munitions Industry Department (MID)**, which controls the DPRK's research and development and productions of weapons—to include nuclear weapons and ballistic missiles—and other military equipment. The MID is subordinate to the Korean Worker's Party Central Committee and, through the 313 General Bureau, deploys a majority of the DPRK's IT work force overseas. All property and interests in property of the Workers' Party of Korea is blocked pursuant to Executive Order (E.O.) 13722.

- **The Ministry of Atomic Energy Industry**—a critical player in the DPRK's development of nuclear weapons and in charge of day-to-day operation of the DPRK's nuclear weapons program. The Ministry of Atomic Energy Industry is designated pursuant to E.O. 13382.

- Military entities subordinate to the **Ministry of Defense and Korea People's Army**. The Korean People's Army is designated on the Specially Designated Nationals and Blocked Property List.

- Lesser-known entities, such as the **DPRK Education Commission's Foreign Trade Office** and the **Pyongyang Information Technology Bureau of the Central Committee's Science and Education Department**. All property and interests in property of the Government of the DPRK is blocked pursuant to E.O. 13722.

An overseas DPRK IT worker earns at least ten times more than a conventional North Korean laborer working in a factory or on a construction project overseas. DPRK IT workers can individually earn

more than USD 300,000 a year in some cases, and teams of IT workers can collectively earn more than USD 3 million annually. A significant percentage of their gross earnings supports DPRK regime priorities, including its WMD program.

DPRK IT companies and their workers normally engage in a wide range of IT development work of varying complexity and difficulty, such as:

- mobile applications and web-based applications,
- building virtual currency exchange platforms and digital coins,
- general IT support,
- graphic animation,
- online gambling programs,
- mobile games,
- dating applications,
- artificial intelligence-related applications,
- hardware and firmware development,
- virtual reality and augmented reality programing,
- facial and biometric recognition software, and
- database development and management.

Applications and software developed by DPRK IT workers span a range of fields and sectors, including business, health and fitness, social networking, sports, entertainment, and lifestyle. DPRK IT workers often take on projects that involve virtual currency. Some DPRK IT workers have designed virtual currency exchanges or created analytic tools and applications for virtual currency traders and marketed their products themselves.

For decades, the DPRK has underscored the importance of education in mathematics and science for its citizens. The emphasis on the advancement of science and technology, which has historically been a priority for the Kim regime, is reflected in the investment of resources and personnel into related fields of research. Today's cyber and IT education in the DPRK was founded on this drive for advancement and resulted in an integrated curriculum coordinated with the Workers' Party, research centers, and the military.

- In recent years under Kim Jong Un, the regime has placed increased focus on education and training in IT-related subjects and has developed strong IT degree programs at several premier DPRK educational institutions—particularly Kim Il Sung University, Kim Chaek University of Technology, and Pyongyang University of Science and Technology. Approximately 30,000 students study information and communications technology-related subjects at these top universities alone.

- As of 2019, 37 universities had reportedly established 85 programs offering courses in advanced science, technology, engineering, and math (STEM) subjects, including information security, and each province had established at least one new secondary school to cultivate promising students.

- The DPRK education system is highly competitive, and only the top students are accepted into the elite science and technology programs. Students are recruited at a young age from secondary schools like Kumsong Academy and Kumsong Middle School Number 1.

- DPRK IT workers receive additional training overseas and from their own organizations, often through regional IT research centers within the DPRK to further develop their skills. DPRK IT workers have historically received training in East Africa, Southeast Asia, and South Asia and benefit considerably from their overseas training.

HOW DPRK IT WORKERS OPERATE

DPRK IT workers target freelance contracts from employers located in wealthier nations, including those in North America, Europe, and East Asia. In many cases, DPRK IT workers present themselves as South Korean, Chinese, Japanese, or Eastern European, and U.S.-based teleworkers.

In some cases, DPRK IT workers further obfuscate their identities by creating arrangements with third-party sub-contractors. These sub-contractors are non-North Korean, freelance IT workers who complete contracts for the DPRK IT workers. DPRK IT managers have also hired their own teams of non-North Korean IT workers who are usually unaware of the real identity of their North Korean employer or the fact that their employer is a DPRK company. The DPRK IT managers use their outsourced employees to make software purchases and interact with customers in situations that might otherwise expose a DPRK IT worker.

Although DPRK IT workers normally engage in non-malicious IT work, such as the development of a virtual currency exchange or a website, they have used the privileged access gained as contractors to enable DPRK's malicious cyber intrusions. Some overseas-based DPRK IT workers have provided logistical support to DPRK-based malicious cyber actors, although the IT workers are unlikely to be involved in malicious cyber activities themselves. DPRK IT workers may share access to virtual infrastructure, facilitate sales of data stolen by DPRK cyber actors, or assist with the DPRK's money-laundering and virtual currency transfers.

DPRK IT workers have also assisted DPRK officials in procuring WMD and ballistic missile-related items for the DPRK's prohibited weapons programs.

There are instances where workers are subjected to human trafficking, including forced labor. Credible reports show many DPRK workers overseas are subjected to excessive work hours, constant and close surveillance by North Korean government security agents, unsafe and unsanitary living

conditions, and little freedom of movement. The North Korean government withholds up to 90 percent of wages of overseas workers which generates an annual revenue to the government of hundreds of millions of dollars.

DPRK IT Workers: Skills and Platforms

DPRK IT teams abroad most commonly obtain freelance jobs through various online platforms. Companies use these platforms to advertise contracts for projects that freelance IT developers can bid on. Less commonly, the DPRK IT teams find local, non-DPRK nationals to serve as the nominal heads of companies that are actually controlled by North Koreans. There have also been instances in which DPRK IT teams appear, on paper, to work for a legitimate local company but pursue their own business independently – and in return for hiding their North Korean origins, the DPRK IT team will pay a fee to the foreign company. DPRK IT teams often include members proficient in a foreign language, such as English or Chinese.

DPRK IT workers use a wide variety of mainstream and IT industry-specific freelance contracting platforms, software development tools and platforms, messaging applications, and social media and networking websites to obtain development contracts for companies around the world, as well as utilizing a number of digital payment platforms and websites to receive payment for their work. DPRK IT workers also use virtual currency exchanges and trading platforms to manage digital payments they receive for contract work as well as to launder and move funds they receive.

DPRK IT Workers: Hiding Their Identity

DPRK IT workers deliberately obfuscate their identities, locations, and nationality online, often using non-Korean names as aliases. They will also use virtual private networks (VPNs), virtual private servers (VPSs), or utilized third-country IP addresses to appear as though they are connecting to the internet from inconspicuous locations and reduce the likelihood of scrutiny of their DPRK location or relationships. DPRK IT workers generally rely on the anonymity of telework arrangements, use proxies for account creation and maintenance, and favor the use of intermediaries and communications through text-based chat instead of video calls.

DPRK IT workers use proxy accounts to bid on, win, work on, and get paid for projects on freelance software developer websites. These proxy accounts belong to third-party individuals, some of whom sell their identification and account information to the DPRK IT workers. In some cases, DPRK IT workers pay fees to these individuals for use of their legitimate platform accounts. DPRK IT workers may populate freelance platform profiles with the real affiliations and work experience of the proxy.

At times, DPRK IT workers engage other non-North Korean freelance workers on platforms to propose collaboration on development projects. A DPRK IT worker takes advantage of these business relationships to gain access to new contracts and virtual currency accounts used to conduct the IT work over U.S. or European virtual infrastructure, bypassing security measures intended to prevent

fraudulent use. In establishing accounts with the aid of other freelance workers, DPRK IT workers may claim to be third-country nationals who need U.S. or other Western identification documents and freelance platform accounts to earn more money.

Hiding their real locations allows DPRK IT workers to violate terms of service agreements for the online platforms and services they use for their activities. As part of their tradecraft, DPRK IT workers may also use single, dedicated devices for each of their accounts, especially for banking services, to evade detection by fraud prevention, sanctions compliance, and anti-money laundering measures.

DPRK IT workers routinely use counterfeit, altered, or falsified documents, including identification documents, and forged signatures—either that they have made themselves using software such as Photoshop, or that they have paid a document forgery company to alter, combining the IT worker's own or a provided photo with the identifying information of a real person. DPRK IT workers commonly procure forged documents such as:

- driver's licenses,
- social security cards,
- passports,
- national identification cards,
- resident foreigner cards,
- high school and university diplomas,
- work visas, and
- credit card, bank, and utility statements.

In some instances, these identities are stolen, while in others the DPRK IT workers have solicited a non-North Korean national to set up an account using their own personal information or information to which they have access, after which control of the account is transferred to the DPRK IT workers for a fee. This allows the DPRK IT worker to conceal their identity when bidding on and completing freelance projects for clients online, using the infrastructure of the real account holder via remote desktop access. Each IT worker often uses multiple identities and accounts, which can also be shared between IT workers on the same team. These accounts and identities purport to be from countries from every part of the world.

DPRK IT workers may steal the customer account information of U.S. or international banks to verify their identities with freelance platforms, payment providers, and companies employing the DPRK IT workers. In at least one case, DPRK IT workers forged checks using stolen bank account information. Accounts and resumes associated with DPRK IT worker's proxy identities often include falsified, but realistic and detailed education and employment history information, including false contact information for educational institutions and previous employers.

DPRK IT workers may also populate their online developer profiles' employment sections with the names of small or mid-sized Western companies so that the DPRK IT workers appear to be reputable Americans or Europeans when bidding on projects. They may use the names of actual employees and email addresses that appear similar to the Western company's legitimate domain.

DPRK IT workers additionally falsify statement of work agreements, invoices, client communication documentation, and other documents for use with freelancing platforms, likely to satisfy know-your-customer and anti-money laundering (KYC/AML) measures or similar procedures that platforms have in place to ensure the legitimacy of user activity. These falsified documents may have minimal contact details to deter verification.

DPRK IT workers may also attempt to mask their nationality by representing themselves as South Korean or simply "Korean" citizens.

DPRK IT workers who obtain freelance positions with an unwitting company have also been known to subsequently recommend to the company the freelance employment of additional DPRK IT workers.

Resume of a DPRK IT Worker

DPRK IT workers advertise skills working on system and program development, database management systems, and use of a wide variety of common languages, frameworks, tools, and cloud resources. These often include strong skills in a number of coding and markup languages. A majority of DPRK IT worker projects are related to mobile and web app development. DPRK IT workers also use collaborative platforms and hosting services for data and workflow management. These workers often report experience with a variety of databases and are familiar with the cloud and analytics products and services from major providers. Additionally, DPRK IT workers incorporate digital payment and e-commerce platforms in their work.

DPRK IT workers build "portfolio" websites, generally simple in design, in an effort to boost the credibility of their fabricated, freelance developer personas. These virtual portfolios represent the work of DPRK IT workers' personas and are often linked to their online freelance developer accounts. Information on these websites, including contact information and location, as well as work history and education, is likely to be false.

RED FLAG INDICATORS

Freelance work and payment platform companies should be aware of the following activity that may be indications or behaviors of DPRK IT workers who may be using their platforms.

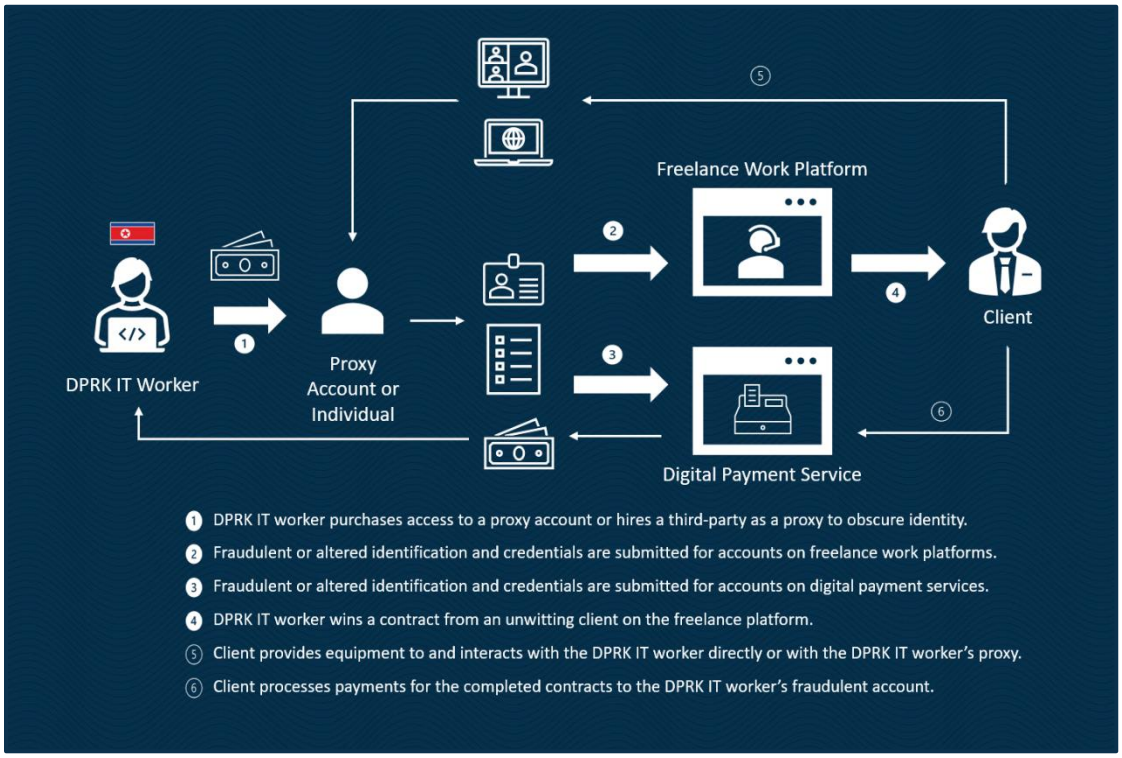
- Multiple logins into one account from various IP addresses in a relatively short period of time, especially if the IP addresses are associated with different countries;
- Developers are logging into multiple accounts on the same platform from one IP address;
- Developers are logged into their accounts continuously for one or more days at a time;
- Router port or other technical configurations associated with use of remote desktop sharing software, such as port 3389 in the router used to access the account, particularly if usage of remote desktop sharing software is not standard company practice;
- Developer accounts use a fraudulent client account to increase developer account ratings, but both the client and developer accounts use the same PayPal account to transfer/withdraw money (paying themselves with their own money);
- Frequent use of document templates for things such as bidding documents and project communication methods, especially the same templates being used across different developer accounts;
- Multiple developer accounts receiving high ratings from one client account in a short period, with similar or identical documentation used to establish the developer accounts and/or the client account;
- Extensive bidding on projects, and a low number of accepted project bids compared to the number of projects bids on by a developer; and
- Frequent transfers of money through payment platforms, especially to PRC-based bank accounts, and sometimes routed through one or more companies to disguise the ultimate destination of the funds.

Companies employing freelance developers should be aware of the following activity that may be indications or behaviors of DPRK IT workers.

- If a freelance software development website or payment platform account has been shut down or the worker contacts the employer requesting use of a different account, especially if registered to a different name;
- Use of digital payment services, especially PRC-linked services;

- Inconsistencies in name spelling, nationality, claimed work location, contact information, educational history, work history, and other details across a developer's freelance platform profiles, social media profiles, external portfolio websites, payment platform profiles, and assessed location and hours;
- Surprisingly simple portfolio websites, social media profiles, or developer profiles;
- Direct messaging or cold-calls from individuals purporting to be C-suite level executives of software development companies to solicit services or advertise proficiencies;
- Requests to communicate with clients and potential clients on a separate platform than the original freelance platform website where the client found the IT worker;
- An employer proposes to send documents or work-related equipment such as a laptop to a developer, and the developer requests that items be sent to an address not listed on the developer's identification documentation. Be particularly suspicious if a developer claims they cannot receive items at the address on their identification documentation;
- Seeking payment in virtual currency in an effort to evade KYC/AML measures and use of the formal financial system;
- Requesting payment for contracts without meeting production benchmarks or check-in meetings;
- Inability to conduct business during required business hours;
- Incorrect or changing contact information, specifically phone numbers and emails;
- Biographical information which does not appear to match the applicant;
- Failure to complete tasks in a timely manner or to respond to tasks;
- Inability to reach them in a timely manner, especially through "instant" communication methods; and
- Asking co-workers to borrow some of their personal information to obtain other contracts.

Overview of DPRK IT Worker Operations



POTENTIAL MITIGATION MEASURES

For freelance work and payment platform companies

- Verify documents submitted as part of proposal reviews and contracting due-diligence procedures, such as independently verifying invoices and work agreements by contacting the listed clients using contact information given in business databases and not the contact information provided on the submitted documentation;

- Closely scrutinize identity verification documents submitted for forgery, potentially reaching out to local law enforcement for assistance. Reject low-quality images submitted to provide verification of identity;

- Verify the existence of any websites provided to establish accounts; enhance scrutiny for any accounts that have utilized defunct websites to establish the accounts.

- As part of initial due diligence contracting processes and refresh policies, require submission of a video verifying identity or conduct a video interview to verify identity;

- Regularly use port checking capabilities to determine if the platform is being accessed remotely via desktop sharing software or a VPN or VPS, particularly if usage of remote desktop sharing software or VPN services to access accounts is not standard practice;

- Automatically flag for additional review client and developer accounts that use the same or similar documentation to establish the accounts or that use the same digital payment service accounts;

- Automatically flag for additional review the use of the same or similar document templates for bidding and project communication across different developer accounts;

- Automatically flag for additional review multiple developer accounts receiving high ratings from a single client account in a short period, especially if similar or identical documentation was used to establish the accounts;

- Automatically flag for additional review developer accounts with high bidding rates as well as accounts with a low number of accepted project bids compared to the number of project bids. Additionally, flag accounts with a high number of project bids relative to number of account logins;

- Do not allow any activity in newly established accounts prior to full account verification;

- Provide extra scrutiny to newly established accounts; and

For companies hiring programmers and developers on freelance platforms

- Conduct video interviews to verify a potential freelance worker's identity;

- Conduct a pre-employment background check, drug test, and fingerprint/biometric log-in to verify identity and claimed location. Avoid payments in virtual currency and require verification of banking information corresponding to other identifying documents;

- Use extra caution when interacting with freelance developers through remote collaboration applications, such as remote desktop applications. Consider disabling remote collaboration applications on any computer supplied to a freelance developer;

- Verify employment and higher education history directly with the listed companies and educational institutions, using contact information identified through a search engine or other business database, not directly obtained from the potential employee or from their profile;

- Check that the name spelling, nationality, claimed location, contact information, educational history, work history, and other details of a potential hire are consistent across the developer's freelance platform profiles, social media profiles, external portfolio websites, payment

platform accounts, and assessed location and hours of work. Be extra cautious of simple portfolio websites, social media profiles, or developer profiles;

- Be cautious of a developer requesting to communicate on a separate platform outside the original freelance platform website where a company initially found the IT worker;
- If sending to a developer documents or work-related equipment such as a laptop, only send to the address listed on the developer's identification documents and obtain additional documentation if the developer requests that the laptop or other items be sent to an unfamiliar address. Be suspicious if a developer cannot receive items at the address on their identification documentation; and
- Be vigilant for unauthorized, small-scale transactions that may be fraudulently conducted by contracted IT workers. In one case, DPRK IT workers employed as developers by a U.S. company fraudulently charged the U.S. company's payment account and stole over USD 50,000 in 30 small installments over a matter of months. The U.S. company was not aware the developers were North Korean or of the ongoing theft activity due to the slight amounts.

CONSEQUENCES OF ENGAGING IN PROHIBITED OR SANCTIONABLE CONDUCT

Individuals and entities engaged in or supporting DPRK IT worker-related activity, including processing related financial transactions, should be aware of the potential legal consequences of engaging in prohibited or sanctionable conduct.

UN Security Council resolutions 2321, 2371, and 2397 highlight that the revenue generated from overseas DPRK workers contributes to the DPRK's nuclear weapons and ballistic missile programs. UN Security Council resolution 2375 prohibits UN Member States from providing new work authorizations, or renewing expired authorizations, for DPRK nationals in their jurisdictions in connection with admission to their territories unless approved in advance by the UN Security Council's 1718 Committee. UN Security Council resolution 2397 requires all Member States to repatriate, by December 22, 2019, DPRK nationals earning income in their jurisdiction—regardless of when or whether work authorizations were issued for the DPRK nationals in question.

The Department of the Treasury's Office of Foreign Assets Control (OFAC) has the authority to impose financial sanctions on any person determined to have, among other things:

- Engaged in significant activities on behalf of the Government of the DPRK or the Workers' Party of Korea that undermine cybersecurity;
- Operated on behalf of the DPRK in the IT industry;
- Engaged in certain other malicious cyber-enabled activities;

- Engaged in at least one significant importation from or exportation to the DPRK of any goods, services, or technology;

- Sold, supplied, transferred, or purchased, directly or indirectly, to or from the DPRK or any person acting for or on behalf of the Government of the DPRK or the Workers' Party of Korea, software, where any revenue or goods received may benefit the Government of the DPRK or the Workers' Party of Korea; or

- Materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, the Government of the DPRK or the Workers' Party of Korea.

For example, in 2018, the United States designated for sanctions the China-based technology firm Yanbian Silverstar Network Technology Co., Ltd. This company was nominally a Chinese IT company, but in reality it was managed and controlled by North Koreans. This company also created a Russia-based front company, Volasys Silver Star, to circumvent identification requirements on freelance job forums.

Additionally, if the Secretary of the Treasury, in consultation with the Secretary of State, determines that a foreign financial institution has knowingly conducted or facilitated significant trade with the DPRK, or knowingly conducted or facilitated a significant transaction on behalf of a person designated under a DPRK-related Executive Order, or under Executive Order 13382 (Weapons of Mass Destruction Proliferators and Their Supporters) for DPRK-related activity, that institution may, among other potential restrictions, lose the ability to maintain a correspondent or payable-through account in the United States.

OFAC investigates apparent violations of its sanctions regulations and exercises enforcement authority, as outlined in the Economic Sanctions Enforcement Guidelines, 31 C.F.R. part 501, appendix A. Persons who violate the North Korea Sanctions Regulations, 31 C.F.R. part 510, may face civil monetary penalties of up to the greater of the applicable statutory maximum penalty or twice the value of the underlying transaction.

In addition, the Countering America's Adversaries Through Sanctions Act (CAATSA; Public Law 115-44) Section 321(b) (22 U.S.C. § 9241a), which amended the North Korea Sanctions and Policy Enhancement Act of 2016 (22 U.S.C. § 9241 et seq.), created a rebuttable presumption that significant goods, wares, merchandise, and articles mined, produced, or manufactured wholly or in part by North Korean nationals or North Korean citizens anywhere in the world are forced-labor goods prohibited from importation under the Tariff Act of 1930 (19 U.S.C. § 1307). This means that these goods shall not be entitled to entry at any port of the United States and may be subject to detention, seizure, and forfeiture. Violations may result in civil penalties, as well as criminal prosecution. However, pursuant to CAATSA, such goods may be imported into the United States if the Commissioner of U.S. Customs and Border Protection (CBP) finds by clear and convincing evidence that the goods were not

produced with convict labor, forced labor, or indentured labor. The prohibition against the importation of goods produced with convict labor, forced labor, or indentured labor under penal sanctions (including forced or indentured child labor) was created under the Tariff Act of 1930, and as such, has been in place for nearly 90 years.

The Department of Justice is responsible for the investigation and prosecution of applicable federal laws, including the International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. §§ 1701 et seq., and the Bank Secrecy Act (BSA), 31 U.S.C. §§ 5318 and 5322. Under IEEPA, it is a crime to willfully violate, attempt to violate, conspire to violate, or cause a violation of any license, order, regulation, or prohibition issues pursuant to IEEPA, to include any DPRK-related Executive Order (e.g., Executive Orders 13722 and 13810), Executive Order 13382, and the North Korean Sanctions Regulations, 31 C.F.R. part 510. Persons who willfully violate IEEPA face up to 20 years' imprisonment, fines of up to $1 million or totaling twice the gross gain, whichever is greater, and potential forfeiture of all funds involved in such transactions. The BSA requires financial institutions to, among other things, maintain effective anti-money laundering programs and file certain reports with FinCEN. Persons violating the BSA may face up to 5 years' imprisonment, a fine of up to $250,000, and potential forfeiture of property involved in such violations. Corporations and other entities that violate IEEPA, the BSA, and other applicable federal laws may also be criminally prosecuted. The Department of Justice also works with foreign partners to share evidence in support of criminal investigations and prosecutions in the United States and abroad.

Pursuant to 31 U.S.C. § 5318(k), the Secretary of the Treasury or the Attorney General may subpoena a foreign financial institution that maintains a correspondent bank account in the United States for records stored overseas. Where the Secretary of the Treasury or Attorney General provides written notice to a U.S. financial institution that a foreign financial institution has failed to comply with such a subpoena, the U.S. financial institution must terminate the correspondent banking relationship within ten business days. Failure to do so may subject the U.S. financial institutions to daily civil penalties.

DPRK REWARDS FOR JUSTICE

If you have information about illicit DPRK activities in cyberspace, including past or ongoing operations, providing such information through the Department of State's Rewards for Justice program could make you eligible to receive an award of up to $5 million. For further details, please visit https://rewardsforjustice.net/index/?north-korea=north-korea.

ANNEX

United Nations Panel of Experts Reporting on DPRK IT Workers

The UN Security Council 1718 Sanctions Committee on the DPRK is supported by a Panel of Experts (the Panel) who gather, examine, and analyze information from UN Member States, relevant UN bodies, and other parties on the implementation of the measures outlined in the UN Security Council Resolutions addressing the DPRK. The Panel also makes recommendations on how to improve sanctions implementation by providing both a midterm and a final report to the 1718 Committee. These reports can be found at:
https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports

The Panel has investigated multiple cases of DPRK IT workers, such as those subordinate to the UN-designated Munitions Industry Department (MID), and presented information on these investigations in the Panel's semi-annual reports, including the following:

The Panel first reported on DPRK IT workers in its 2019 Midterm Report, noting that the MID, which had been designated for its supervisory role in the development of the DPRK's nuclear and ballistic missile programs, was using its subordinate trading corporations to station abroad DPRK information technology workers, such as software programmers and developers, in order to earn foreign currency. At the time, DPRK IT workers located in Europe, Asia, Africa, and the Middle East utilized foreign websites to obtain freelance work while disguising their identities. Alongside non-malicious information technology work, DPRK IT workers conducted illicit work involving the theft of assets such as virtual currencies in support of DPRK cyber actors in the evasion of financial sanctions.

The Panel continued its investigation into DPRK IT workers in its 2020 Final Report, finding that most overseas DPRK IT workers are employed by companies subordinate to MID. By 2019, the MID was suspected of having dispatched at least 1,000 IT workers overseas for the purpose of revenue generation, often using subordinate entities or front companies. However, due to their obfuscation techniques, the true number of IT workers abroad and in the DPRK was unclear. The Panel noted that DPRK IT workers use several methods to obtain freelance IT work without revealing their identity, including by setting up accounts on freelance developer platforms with unwitting clients around the world, especially in China, Russia, Ukraine, Serbia, Canada, and the United States. The Panel further investigated several specific cases of DPRK IT worker teams and associated companies in China, Nepal, and Vietnam.

The Panel investigated a number of DPRK IT worker teams in China and Russia, detailing their investigations in its 2020 Midterm Report. The Panel noted that hundreds of DPRK IT workers subordinate to MID were operating in China in 2019 and 2020, illicitly gaining access to freelance platform accounts in the names of third-country individuals. The Panel further noted that multiple groups of DPRK MID-subordinate IT workers were operating in Russia in 2019 and 2020, utilizing

false, foreign identities to access information technology freelance platforms, virtual currency websites, and payment websites.

According to the Panel's 2021 Final Report, DPRK IT workers can evade employers' due diligence efforts and KYC/AML protocols by employing similar obfuscation methods as those utilized by the DPRK to access the international financial system, including providing false identification, use of VPN services, and establishing front companies. The Panel further noted that most accounts linked to the DPRK operate from locations in China. To avoid scrutiny, these accounts will go "off-site" after establishing contact with potential customers seeking to hire IT services. DPRK-linked users also target IT freelance platforms with lower levels of security or less rigorous due diligence procedures. The Panel specifically highlighted the dangers facing IT freelance platforms in performing compliance obligations and unintentionally facilitating DPRK access to international payment systems, recommending that UN Member States work with freelance IT companies to promote and enhance sanctions compliance implementation capacity and capability.