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:**
	:	
OLEKSANDR DIDENKO,	:	**18 U.S.C. §§ 1343, 1349 (Conspiracy to Commit Wire Fraud)**
	:	
also known as	:	**18 U.S.C. § 371 (Conspiracy to Defraud the United States & Conspiracy to Commit a Crime)**
ALEXANDER DIDENKO,	:	
	:	
Defendant.	:	**18 U.S.C. § 911 (Falsely Presenting to be a Citizen of the United States)**
	:	
	:	**18 U.S.C. § 1028A(a)(1) (Aggravated Identity Theft)**
	:	
	:	**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)**
	:	
	:	**8 U.S.C. § 1324a (Unlawful Employment of Aliens)**
	:	
	:	**18 U.S.C. §§ 1956(a)(1)(B)(i), (a)(2)(A) & (h) (Conspiracy to Launder Monetary Instruments)**
	:	
	:	**18 U.S.C. § 1960 (Prohibition of Unlicensed Money Transmitting Business)**
	:	
	:	**18 U.S.C. § 2 (Aiding and Abetting)**
	:	

INDICTMENT

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

COUNT ONE
(Conspiracy to Commit Wire Fraud)

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. Hundreds of DPRK IT workers were dispatched to China, illicitly gaining access to freelance platform accounts in the names of third-country individuals.

3. According to the May 2022 advisory, all DPRK IT workers earn money to support the North Korean 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. DPRK entities dispatching IT workers include: (i) 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; (ii) 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; and (iii) military entities subordinate to the Ministry of Defense and Korea People's Army.

4. According to a March 2024 United Nations Security Council Panel of Experts Report, DPRK information technology workers are allowed to keep only a small percentage of their earnings, with the remainder taken by their dispatching DPRK government agency. It is estimated that there are thousands of information technology workers sent overseas from DPRK. Additionally, approximately 1,000 DPRK IT workers operate from cities inside North Korea, including from Shinuiju, a city on the border with Dandong, China.

5. From at least in or around 2018 until May 10, 2024, OLEKSANDR DIDENKO and others known and unknown to the grand jury engaged in a coordinated conspiracy with overseas IT workers, including North Korean IT workers, to (i) create fraudulent accounts under false identities with online freelance IT job search platforms and money service transmitters (MSTs) in order to facilitate work at U.S. companies under those false identities, and (ii) assist the overseas IT workers in performing work at U.S. companies under the false identities through the use of "laptop farms"—U.S. locations that received and hosted laptops issued by U.S. companies to the overseas IT workers, so that the companies believed the workers to be physically located within the United States.

6. DIDENKO's business, UpworkSell, created approximately 869 false proxy identities, which were used to create approximately 2,663 false proxy accounts at U.S.-based

entities, including U.S. freelance IT job platforms, MSTs operating in the United States, and U.S. email and social media providers. Certain of these false proxy identities used identity information of actual U.S. citizens, thereby making it appear that they were eligible for employment in the United States. DIDENKO not only provided false information to these account providers when he created the accounts, the accounts thereafter were the tools and means for overseas IT workers, including North Korean IT workers, to masquerade as U.S. citizens and obtain employment under false pretenses at U.S. companies. DIDENKO further monetized his scheme by convincing U.S.-based friends and associates to host computers for the overseas IT workers at U.S. laptop farms, so that companies in the United States would believe the hired IT workers were in fact performing work from within the United States. DIDENKO was also the key facilitator for UpworkSell's hundreds of "customers." He personally engaged in thousands of communications with customers, many of whom DIDENKO believed were North Korea IT workers, and knowingly assisted and conspired with them in perpetrating fraud.

BACKGROUND

A. Sanctions Against North Korea

7. 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.

8. 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 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. Under EO 13722 and the regulations passed thereto (31 C.F.R. § 510.101 *et seq*. (amended 83 Fed. Reg. 9182 (Mar. 5, 2018)), U.S. persons and entities are generally prohibited the exportation and re-exportation of goods, services (including financial services), and technology to or for the benefit of North Korean entities or individuals, unless exempt or authorized by the Department of the Treasury.

9. The Bank Secrecy Act requires money service businesses, to include MSTs, operating in the United States to take anti-money laundering measures to ensure that U.S. 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 could result in civil and criminal penalties for U.S. money services businesses. As a result of the North Korea sanctions, the FinCEN 311 action, and overall risk management, beginning in at least March 2016,

money service businesses operating in the United States refused to knowingly process any U.S. transactions involving North Korean entities or individuals.

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

10. The Department of Homeland Security ("DHS"), U.S. Citizenship and Immigration Services ("USCIS") is the federal agency responsible for confirming 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 have the employee prepare a 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, the employee must attest to their U.S. citizenship or immigration status, which determines their eligibility for employment. The employee must also present their employer with acceptable documents as evidence of identity and employment eligibility. 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).

b. As a voluntary addition 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, either confirming the employee's employment eligibility or indicating that further information is required. Although E-

Verify requires the use of a photographic identity document, it does not have the ability to compare a submitted state drivers' license photographs against the photographs in 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.

11. The Internal Revenue Service ("IRS") is the federal agency responsible for collection of taxes from U.S. employers and employees and 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.

12. The Social Security Administration ("SSA") is the federal agency responsible for administering retirement, disability, survivor, and family benefits, and is located in the District of Columbia. SSA provides Social Security Numbers, which are unique identifiers that are used to check 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 AND OTHER INDIVIDUALS

13. Defendant OLEKSANDR DIDENKO, also known as "Alexander Didenko" (DIDENKO), is a Ukrainian national, last known to reside in Kyiv, Ukraine. At all times relevant to this Indictment, DIDENKO ran UpworkSell, a business that purported to provide services to remote IT workers and utilized the website https://upworksell.com. DIDENKO engaged at least three employees to run this business: Employee 1 (the "Technical Manager"); Employee 2 (the "Finance Manager"); and Employee 3 (the "Help Desk Manager"). UpworkSell conducted business through at least eight laptop farms, including at locations in Virginia, Tennessee, California, Florida, Ecuador, Poland, and Ukraine. At all times relevant to this Indictment, DIDENKO knew that the individuals with whom he conspired to create false accounts and to facilitate remote IT work through laptop farms were non-U.S. nationals, who were not located in the United States and not authorized to work in the United States. Since at least mid-2022, DIDENKO believed that many of the customers of UpworkSell were likely North Koreans, and knew that many of the customers were located in China, near the North Korean border. DIDENKO received communications from his customers that showed that many of his customers were organized and communicated with each other, including being told by a customer that DIDENKO was working for their "agency," which had "2000 members."

14. Individual 1, a Ukrainian citizen legally residing in the United States, ran a laptop farm for DIDENKO located in Virginia Beach, Virginia. Individual 1 knew Didenko since approximately 2016 when they met in Ukraine, and recruited Individuals 3 and 4 to assist Didenko.

15. Individual 2, a Columbian citizen residing in the United States, ran a laptop farm for DIDENKO located in Jefferson City, Tennessee. Individual 2 also assisted Individual 3 in their work for DIDEKNO running a separate laptop farm.

16. Individual 3, a foreign national legally residing in the United States, ran a laptop farm for DIDENKO located in Tennessee. Individual 3 knew Didenko since approximately 2016 when they met in Ukraine. Individual 3 recruited Individual 2 to assist in running the Tennessee laptop farm.

17. Individual 4 a foreign national legally residing in the United States, ran a laptop farm for DIDENKO located in California.

18. Individual 5, also known as "Piety," was an overseas IT worker and a regular customer of DIDENKO. Piety worked with other overseas IT workers and introduced numerous other overseas IT workers to DIDENKO. Piety caused laptop computers to be shipped from the United States to Dandong, China, a city on the border of Shinuiju, North Korea, addressed to JOHN DOE 3, alias 春姬 金 Chunji JIN (JIN), who Piety said was his "sister." JIN used two U.S.-based MSTs, one of which listed her address as Dandong, China.

JURISDICTION AND VENUE

19. 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.

20. 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

21. Between at least in or around 2018, the exact date being unknown to the Grand Jury, until on or about May 10, 2024, DIDENKO 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. IT job sharing platforms, U.S. MSTs, U.S. company employers, and DHS through the transmission of false information, *to wit*, (i) the conspirators used the identities of other persons to present false information in order to create accounts for overseas IT workers under false identities, which were used to defraud U.S. IT job sharing platforms, U.S. MSTs, U.S. company employers, and some of which were used to verify that overseas IT workers were eligible for employment in the United States and were forwarded to DHS for verification, and (ii) assisted and facilitated overseas IT workers in performing remote work through U.S. based laptop farms and thus falsifying the overseas IT workers actual locations, 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 caused to be transmitted by means of wire communication in interstate commerce the signals and sounds as described herein.

22. The goals and purposes of the Conspiracy were, among others, to obtain online accounts, including with U.S. based providers, for overseas IT workers through the use of false, borrowed, or stolen identities, to obtain U.S.-based jobs for overseas IT workers through the use of the same accounts, to defraud U.S.-based employers as to the location and identity of the overseas IT workers, to generate revenue for the overseas IT workers and their associates, and to generate revenue for DIDENKO.

Manner and Means

23. 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. DIDENKO advertised for UpworkSell's services via a website, with a domain hosted in the United States;

b. DIDENKO created accounts at IT job sharing platforms, MSTs, email providers, and social media providers, including entities based in the United States, through using the means of identification of other persons;

c. DIDENKO sold or rented the aforementioned accounts to coconspirator overseas IT workers, including North Korean IT workers;

d. Coconspirator overseas IT workers using the accounts created by DIDENKO, applied for and obtained jobs at U.S. companies through the provision of false information;

e. DIDENKO and his coconspirators created and managed laptop farms at multiple locations, including at least four locations in the United States, wherein they hosted laptops issued by U.S. companies to coconspirator overseas IT workers;

f. Coconspirator overseas IT workers paid DIDENKO for the aforementioned services through U.S. MSTs using various electronic means using wires in interstate commerce;

g. DIDENKO and the coconspirators communicated with each other through various electronic means, i.e., wires in interstate commerce, including by using U.S.-based service providers.

Overt Acts

24. 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:

- ***Creation of False Proxy User Accounts***

a. Between in or around 2018, until on or about May 10, 2024, DIDENKO and his coconspirators created, including through the use of wire communications in interstate or foreign commerce, 869 "proxy identities," which used the means of identification of another person, which he thereafter associated with accounts at U.S. and overseas providers and MSTs, as described below ("false proxy accounts") and facilitated the same through the use of false identity documents that also used the means of identification of another person, and the accounts were later sold to UpworkSell customers:

Provider	**Number of False Proxy Accounts**
U.S. Platform-1	376
U.S. Platform-2	48
Overseas Platform-1	220
U.S. MST-1	33
U.S. MST-2	605
Overseas MST-1	38
U.S. Email Provider-1	704
U.S. Email Provider-2	126
U.S. Email Provider-3	30
U.S. Email Provider-4	6
U.S. Company 14	4
U.S. Company 15	8
Overseas Company 1	23
Overseas Platform 2	6

U.S. Platform 3	67
Overseas Company 4	1
U.S. Company 16	115
U.S. Company 17	121
U.S. Company 18	4
U.S. Company 19	2
U.S. Company 20	131
Total	***2663***

- ***UpworkSell Website***

b. On or about September 6, 2021, DIDENKO registered the website for his company, UpworkSell, with a U.S. provider through a wire communication in interstate commerce. The website advertised the ability for remote IT workers to buy or rent accounts in the name of identities other than their own:

i. on online freelance IT job platforms, which allow users to advertise thereon as "gig" workers, *i.e.*, to create free accounts, advertise their skills, and bid on IT work contract including: (1) "U.S. Platform-1", located in California; (2) "U.S. Platform-2", located in Pennsylvania; and (3) "Overseas Platform-1," located abroad;

ii. on online MSTs, which 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 online, including: (1) "U.S. MST-1", located in California; (2) "U.S. MST-2", located in New York; and (3) "Overseas MST-1", located abroad but operating in New York for U.S. dollar transactions;

iii. for "Credit Cards" located in the United States and Europe; and

iv. for Subscriber Identity Module ("SIM") cards for cellular phones located in Ukraine.

- ***DIDENKO's Connection to North Korean IT Workers & Other Enablers***

c. 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 an IT worker scheme in an online repository. These files included documents about how to circumvent U.S. laws regarding employment eligibility and obtain employment in the United States as remote workers, including guides and tips related to topics about writing a cover letter and building a resume, sample resumes, scripts for interviews, a scanned copy of a stolen U.S. Permanent Resident Card, and various other files. Included in these documents were:

i. A document titled "Account Sellers," which listed DIDENKO as one of the six "account sellers" used by this North Korean IT Worker group, and included DIDENKO's contact information (email, phone, and social media accounts).

ii. 59 job postings, including three postings for jobs at U.S. companies that were later filled by North Korean IT Workers posing as U.S. persons and operating through a laptop farm run by U.S. citizen CHRISTINA CHAPMAN. CHAPMAN also hosted computers for at least three additional U.S. person identities associated with this same group of North Korean IT workers.

d. Between approximately in or about August 2018 and in or about May 2022, approximately 24 coconspirator overseas IT workers with U.S. MST-2 accounts based in Dandong, China, a city on the border of Shinuiju, North Korea, sent

DIDENKO approximately 175 payments, including through wire communications in interstate commerce, in furtherance of the scheme.

e. On or about November 30, 2021, DIDENKO's coconspirator customer, Piety, exchanged communications via wires in interstate commerce with CHAPMAN and asked CHAPMAN to deposit into a bank account at a U.S. financial institution a paycheck issued in the name of a U.S. person issued for work done by an overseas IT worker at the U.S. company. Piety told CHAPMAN that the bank account was in the name of "Anastasiia [D.]", a purported Ukrainian national and the same identity used by DIDENKO to create a false proxy identity account at U.S. MST-2.

f. Between on or about October 10, 2022, and on or about March 29, 2023, DIDENKO's coconspirator customer Piety requested CHAPMAN ship laptop computers from U.S. businesses to JOHN DOE 3, alias CHUNJI JIN, in Dandong, China, which CHAPMAN did ship on approximately 21 occasions.

g. On or about February 2, 2023, DIDENKO's coconspirator customer Piety instructed CHAPMAN to ship a laptop computer to a shipping service access point in Virginia, for pick up by Individual 1, working at DIDENKO's Virginia laptop farm.

h. On or about October 3, 2023, a conspirator IT worker and customer of DIDENKO's ("Customer-7") stated that they were unhappy with the service at DIDENKO's laptop farm and instructed DIDENKO to send a laptop issued by a U.S. Company from DIDENKO's Virginia laptop farm to CHAPMAN.

- ***Sale and Use of Proxy False Accounts, Utilizing Wires in Interstate Commerce***

i. On or about the following dates, DIDENKO exchanged communications with UpworkSell customers (*i.e.*, the overseas IT workers) through wire communications in interstate commerce about the sale of false proxy accounts:

Customer-1

i. On or about January 30 2020, DIDENKO exchanged communications via wires in interstate commerce with a coconspirator 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."

Customer-2

ii. On or about December 13, 2022, Didenko exchanged communications via wires in interstate commerce with a coconspirator customer ("Customer-2") noting the terms of his account sales, "The payment date is fixed on the 13th of each month. . . . I am glad to introduce you to my financial manager [Employee 2]. 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."

Customer-3

iii. On or about June 7, 2021, DIDENKO exchanged communications via wires in interstate commerce with a coconspirator customer ("Customer-3"), with DIDENKO stating, "Hi! Do you need freelancer com acc[ount]?" Customer-3 responded, "Yeah, I need . . . . Can you show me your account?" DIDENKO then provided his terms of service, to include a 3-day trial period for new clients, followed by a $50 prepayment, and a monthly payment of $90.

Customer-4

iv. On or about May 31, 2023, DIDENKO exchanged communications via wires in interstate commerce with a coconspirator customer ("Customer-4"), who requested to rent a U.S. Platform-1 account. DIDENKO responded, "we can help . . . . We recommend only Ukraine now. it's more safety [sic] . . . ." 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 [U.S. dollar 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."

v. 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 B."

vi. 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, the identity of a U.S. citizen] 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. . . . 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."

vii. On or about June 2, 2023, DIDENKO or a coconspirator registered an account at U.S. MST-2 in U.S. Person-1's name, with a U.S.-based email address and a Ukrainian passport.

viii. On or about June 6, 2023, DIDENKO sent Customer-4 U.S. MST-2 login information for an account associated with U.S. Person-1.

ix. On or about August 28, 2023, Customer-4 exchanged communications via wires in interstate commerce with 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$".

x. On or about August 30, 2023, DIDENKO or a coconspirator registered an account at U.S. MST-2 in U.S. Person-1's name, with a U.S.-based email address and a Ukrainian passport, with a different photo than used on June 2, 2023, but an identical signature.

xi. On or about September 5, 2023, DIDENKO sent to Customer-4 U.S. MST-2 login information for an account associated with U.S. Person-1.

xii. Between on or about October 27, 2023, Customer-4 exchanged communications via wires in interstate commerce with DIDENKO, "I request one more [U.S. MST-2] with [U.S. Person-1]".

xiii. On or about October 28, 2023, DIDENKO or a coconspirator registered an account at U.S. MST-2 in U.S. Person-1's name, with a U.S.-based email address and a Ukrainian passport.

xiv. On or about October 30, 2023, DIDENKO sent to Customer-4 U.S. MST-2 login information for an account associated with U.S. Person-1.

Customer-5

xv. On or about September 28, 2019, DIDENKO exchanged communications via wires in interstate commerce with a coconspirator customer ("Customer-5"), who inquired about his U.S. Platform-1 account, "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? . . . faktme@gmail.com?" To which DIDENKO responded "ok".

Customer-9

xvi. On or about January 2, 2024, DIDENKO exchanged communications via wires in interstate commerce with a coconspirator customer ("Customer-9"), who asked DIDENKO to set up a U.S. MST-2 account in the name "Henry H[.]". DIDENKO responded, "Order accepted" and thereafter sent the login credentials for U.S. Email Provider-1 and for an account at U.S. MST-2 with the same information. DIDENKO stated, "If you want use acc on real safety pc – ping me, we will help with that. 55$ is prepayment, 55$ per/m." Customer-9 responded, "Thanks, Alexander."

j. On or about the following dates, coconspirator overseas IT workers, who were customers of DIDENKO and using accounts created by 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 through wire communications in interstate commerce, *i.e.*, the E-Verify system, in order to verify the overseas IT workers' employment eligibility:

Sub-¶	Date	U.S. Person Identity	Document 1	State	Document 2	Employer
i.	7/19/2023	U.S. Person-1	State Driver's License/ID	TX	Social Security (SS) Card	U.S. Company-7
ii.	11/13/2023	U.S. Person-1	State Driver's License/ID	TX	SS Card	U.S. Company-6
iii.	1/2/2024	U.S. Person-2	State Driver's License/ID	PA	SS Card	U.S. Company-2
iv.	1/9/2024	U.S. Person-2	State Driver's License/ID	PA	SS Card	U.S. Company-8

v.	2/21/2024	U.S. Person-2	State Driver's License/ID	PA	SS Card	U.S. Company-4
vi.	2/22/2024	U.S. Person-2	State Driver's License/ID	PA	SS Card	U.S. Company-9
vii.	3/6/2024	U.S. Person-2	State Driver's License/ID	PA	SS Card	U.S. Company-10
viii.	3/13/2024	U.S. Person-2	State Driver's License/ID	PA	Birth Certificate	U.S. Company-11
ix.	9/20/2023	U.S. Person-3	State Driver's License/ID	NY	SS Card	U.S. Company-12

k. On or about the following dates, U.S. Company-5 paid a coconspirator overseas IT worker in the name of U.S. Person-1, and thereafter U.S. Company 5 sent funds in the name of U.S. Person-1 to an account with U.S. MST-2 created by DIDENKO, when in fact the real U.S. Person-1 had not performed such work:

Sub-¶	Date	Amount
i.	9/22/2023	$4,113.60
ii.	10/6/2023	$3,662.49
iii.	10/20/2023	$3,662.49
iv.	11/3/2023	$3,580.47
v.	11/17/2023	$3,662.49
vi.	12/1/2023	$3,334.41
vii.	12/15/2023	$2,999.11
viii.	12/29/2023	$3,662.49
ix.	1/12/2024	$3,352.93
x.	1/26/2024	$3,352.93

- ***Hosting Computers at U.S. Laptop Farms and Conveyance of False Location Information to U.S. Companies Over Wires in Interstate Commerce***

l. Between in or around the following dates, at the direction of DIDENKO, conspirator overseas IT workers caused U.S. companies to send laptops and other devices issued by U.S. companies to DIDENKO's laptop farms, wherein DIDENKO's associates provided remote access to the networks of U.S.-based

companies, through wire communications in interstate commerce, so that it would appear to the U.S. based company that the remote IT workers were physically located at the laptop farm address.

Sub-¶	Date Range	Location	Associate	Approximate Number of Computers
i.	August 2022 until October 2023	Virginia Beach, Virginia	Individual 1	4
ii.	October 2023 until March 2024	Jefferson City, Tennessee	Individual 2	6
iii.	October 2023 until March 2024	Jefferson City, Tennessee	Individual 3	6
iv.	November 2023 until April 2024	San Diego, California	Individual 4	15
			Total	31

m. On or about the following dates, DIDENKO exchanged communications with UpworkSell customers (*i.e.*, the coconspirator overseas IT workers) through wire communications in interstate commerce about the U.S. laptop farms:

Piety

i. Between November 17, 2022, and December 2, 2022, DIDENKO and Piety exchanged communications about DIDENKO hosting Piety's computers in the United States. Piety stated, "Do you have any friend/partner who can support me in US? I need to save laptops and run anydesk on it. There can be many laptops moving forward. . . . It will be over 5-10 laptops after 2 months. [C]urrently, I have 2 supporters now. . . . let me explain . . . I'm getting jobs from US companies with US citizen identity then companies send laptop to work so, our developers will work on it via anydesk or other app – it would be great if the supporter can have enough time or stay in the office/home." DIDENKO responded, "I think we could help with that. we have an office in

the USA (these are apartments), our [U.S. Platform-1] accounts work there. it works on modems. but we have wifi, I think we could work something out. in fact, the guy who works for us in America is very careful, and we are very worried that a stolen computer will not be sent to us. or something like that."

ii. From on or about February 27, 2023, to on or about March 6, 2023, Piety requested that DIDENKO send a computer from the Virginia laptop farm to a location in Dandong, China, in the name of JIN, who Piety described as his "sister."

Customer-2

iii. On or about September 16, 2023, DIDENKO had an exchange with Customer-2, in which Customer-2 asked for help in receiving a computer in the United States. DIDENKO replied by providing the Virginia laptop farm address and the name of Individual 1. Approximately three days later, Customer-2 sent DIDENKO the tracking number for a package being sent to Individual 1 at the Virginia laptop farm. Approximately two days later, DIDENKO responded to Customer-2, "Hi! Your USA PC is activated. We can provide anydesk access. 200$ is prepayment".

iv. On or about October 14 2023, DIDENKO received an inquiry from Customer-2 if he/she could have another computer sent to Individual 1's address (*i.e.*, the Virginia laptop farm). DIDENKO responded, "Ofc you can, but let's use another address" and then provided one of the Tennessee laptop farm addresses and the name of Individual 3. Approximately five days later, Customer-2 exchanged communications via wires in interstate commerce

with DIDENKO with a tracking number for the shipment. The following day, DIDENKO sent a confirmation that the laptop had been picked up.

Customer-3

v. On or about November 22, 2023, Customer-3 sent DIDENKO communications via wires in interstate commerce 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 Customer-3 the address for the California laptop farm and the name of Individual 4. Approximately two weeks later, Customer-3 exchanged communications via wires in interstate commerce with DIDENKO a shipping tracking number for a laptop shipment. Approximately two days later, DIDENKO replied, "The agent informed me 2 minutes ago that we received the package."

Customer-4

vi. On or about June 7, 2023, Customer-4 sent DIDENKO communications via wires in interstate commerce, "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." DIDENKO responded, "We can receive laptop in another state" provided an address for a commercial shipping service's "access point" (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: [Individual 1]". Customer-4 clarified that the company "will ship with [Individual 1's] name . . . and a family member can receive it. I introduced them [Individual 1] is my wife". Approximately three weeks later, DIDENKO provided Customer-4 with remote log-in credentials for the computer.

vii. On or about August 18, 2023, Customer-4 sent the address for the Virginia laptop farm to DIDENKO and asked, "Does this address work for laptop delivery? . . . I provided this address." DIDENKO responded, "yes, sure".

viii. On or about October 2, 2023, DIDENKO sent Customer-4 Individual 2's Tennessee address as the "new" address for laptops.

Customer-7

ix. On or about September 22, 2023, DIDENKO exchanged communications via wire communications in interstate commerce with a coconspirator customer ("Customer-7") about a computer that had been shipped to the Virginia laptop farm.

x. 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."

xi. On or about October 3, 2023, when the laptop had still not been set up at the Virginia laptop farm, 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. [CHAPMAN's Arizona laptop farm address]. In reference to this address, DIDENKO inquired, "Let me know name of receiver also". Customer-7 replied, "Christina Chapman".

xii. On or about October 6, 2023, Customer-7 confirmed to DIDENKO, "I've received laptop and set it up," referring to the laptop's arrival at CHAPMAN's laptop farm.

n. Between approximately in or around August 2022, until on or about May 10, 2024, coconspirator overseas IT workers obtained employment through the fraudulent use of identification, and thereafter performed or attempted to perform remote IT work for at least the following U.S. companies (including through staffing companies), while the laptops provided for this work were hosted by one of DIDENKO's laptop farms:

Sub-¶	U.S Person Identity	Victim Company (if known)	Laptop Location (if sent)
i.	"Arber B."	U.S. Company 21	California
ii.	"Arber B."	U.S. Company 22	California
iii.	"Christopher H."	U.S. Company 23	California
iv.	"Christopher H."	U.S. Company 23	California
v.	"Guazzaloca J." OR "Martin R."	U.S. Company 24	California
vi.	"Harry T."	U.S. Company 25	California
vii.	"Jose H."	U.S. Company 26	California
viii.	"Jose H."	U.S. Company 27	California
ix.	"Jose H."	U.S. Company 28	California

x.	"Josiah K."	U.S. Company 29	California
xi.	"Matthew M."	U.S. Non-profit Company 1	California
xii.	"Micheal J."	U.S. Company 30	California
xiii.	"Raymond S."	U.S. Company 29	California
xiv.	"Trayvon H."	U.S. Company 31	California
xv.	"Trayvon H."	Overseas Company 5	California
xvi.	Unknown	U.S. Company 32	California
xvii.	Unknown	U.S. Company 32	California
xviii.	"Frank P."	U.S. Company 33	Tennessee
ixx.	"Harry P."	U.S. State Agency 1	Tennessee
xx.	"Kevin R."	U.S. Company 34	Tennessee
xxi.	"Matthew M."	U.S. Company 21	Tennessee
xxii.	"Matthew M."	U.S. Company 23	Tennessee
xxiii.	"Matthew M."	U.S. Company 35	Tennessee
xxiv.	"Matthew M."	U.S. Company 36	Tennessee
xxv.	"Matthew M."	U.S. Company 37	Tennessee
xxvi.	"Michael W."	U.S. Company 38	Tennessee
xxvii.	"Victor M."	U.S. Company 39	Tennessee
xxviii.	"Willie E."	[unknown]	Tennessee
ixxx.	Unknown	U.S. Company 40	Tennessee
xxx.	"Harry P."	U.S. Company 41	N/A
xxxi.	"Aaron T."	U.S. Company 42	Virginia
xxxii.	"Aaron T."	U.S. Company 43	N/A
xxxiii.	"Daniel S."	U.S. Company 44	Virginia
xxxiv.	"Raymond S."	U.S. Company 45	Virginia
xxxv.	"Tanya R."	U.S. Company 46	Virginia
xxxvi.	"Willie E."	U.S. Company 12	Virginia

o. Between on or about the following dates, DIDENKO made payments through wire communications in interstate commerce to Individuals 1-3 for their services in

hosting his U.S. laptop farms, usually in the amount of approximately $100 per month:

Sub-¶	Date Range	Associate	Payment Means	Approximate Total
i.	2/3/2023 – 12/20/2023	Individual 1	U.S. MST-1	$1,300
ii.	12/2/2023 – 2/19/2024	Individual 2	U.S. MST-1	$430
iii.	10/20/2023 – 10/31/2023	Individual 3	U.S. MST-1	$58
			Total	***$1,788***

p. Between approximately on or about the following dates, coconspirator overseas IT workers sent DIDENKO U.S. dollar payments, including through wire communications in interstate commerce, for the account creation and rental services and for hosting of laptops at the U.S. laptop farms, through accounts created in DIDENKO's name at the following providers.

Sub-¶	Date Range	Provider	Number of Accounts	Total Payments
i.	03/14/2020 – 12/21/2023	U.S. MST-1	517	$88,348.47
ii.	07/16/2018 – 06/07/2022	U.S. MST-2	2,422	$645,439.62
iii.	12/22/2021 – 12/20/2023	Overseas MST-1	142	$188,946.55
			Total	$922,734.64

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

COUNT TWO

(Conspiracy to Defraud the United States)

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

26. Beginning at in or around 2018, the exact date being unknown to the Grand Jury, through on or about May 10, 2024, DIDENKO 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 commit an offense against the United States, that is to defraud by means of deceit, craft, trickery, and dishonesty the United States and its agencies, by interfering with and obstructing lawful government function, that is, the enforcement of laws and regulations regarding employment, by misrepresenting their identities and their U.S. employment eligibility through the use of accounts created by DIDENKO and the services of DIDENKO's laptop farms, thereby causing U.S. companies to unknowingly transmit false information to the United States and its agencies in the name of U.S. persons as set forth in ¶¶ 24(j) & (n), and caused false information to be transmitted to the following agencies:

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

b. IRS, by submitting false information regarding wages earned by U.S. persons, and thereafter creating false tax liabilities in the name of the U.S. persons; and

c. SSA, by submitting false information regarding benefits earned by U.S. persons and thereafter creating false benefit coverage in the name of the U.S. persons.

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

COUNT THREE

(Conspiracy to Falsely Represent to Be a Citizen of the United States

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

28. Beginning at in or around 2018, the exact date being unknown to the Grand Jury, through on or about May 10, 2024, DIDENKO 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 commit an offense against the United States, *to wit* to falsely represent the overseas IT workers to be citizens of the United States in violation of Title 18, United States Code, Section 911.

(**Conspiracy to Falsely Represent to be a Citizen of the United States**, in violation of Title 18, United States Code, Sections 911, 371)

COUNT FOUR
(Aggravated Identity Theft)

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

30. DIDENKO 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, *to wit* the true names, Social Security numbers, dates of birth, and other identifying information of stolen or otherwise obtained actual person identities, during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), *to wit* conspiracy to commit wire fraud as set forth in Count One and conspiracy to falsely represent to be a U.S. citizen as set forth in Count Three, knowing that the means of identification belonged to another actual person, on or about the dates listed and using the identities listed in ¶¶ 24(j) & (n).

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

COUNT FIVE
(Conspiracy to Commit Fraud in Connection with Identification Documents)

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

32. Between at least in or around 2018, the exact date being unknown to the Grand Jury, and on or about May 10, 2024, DIDENKO 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, *to wit* the names, Social Security numbers, and dates of birth and other identifying information of stolen or otherwise obtained 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, *to wit* conspiracy to commit wire fraud as set forth in Count One and conspiracy to falsely represent to be a U.S. citizen as set forth in Count Three, and as a result of the offense, DIDENKO and the conspirators obtained something of value aggregating $1,000 or more during any 1-year period.

33. 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:

U.S. Person-1

a. In or around August 2023, a coconspirator overseas IT worker associated with Customer-4 and posing as U.S. Person-1, a U.S. citizen, obtained employment at U.S. Company-5. The coconspirator overseas IT worker posing as U.S. Person-1 provided a fake a Texas driver's license and a Social Security card in the name of U.S. Person-1. The fake driver's license used U.S. Person-1's actual name, and date of birth, but pictured an Asian male instead of a photo of the actual U.S. Person-1, which did not match the photo in the Ukrainian passport showing a white male used to create the U.S. MST-2 account in the name of U.S. Person-1. U.S. Company-5 subsequently made payments to the U.S. MST-2 account for this U.S. Person-1 identity, created by DIDENKO.

b. On or about November 13, 2023, a coconspirator overseas IT worker associated with Customer-4, posing as U.S. Person-1, and using U.S. Person-1's identification information obtained employment at U.S. Company-6, a technology staffing company in Maryland, to work on a contract with a government agency. The coconspirator overseas IT worker posing as U.S. Person-1 provided a fake Texas driver's license with a picture of an Asian male, the same ID provided to U.S. Company-5. After being informed that they needed to be fingerprinted for the contract with the government agency, the coconspirator overseas IT worker posing as U.S. Person-1 claimed a health issue and was placed on "disability leave".

c. On or about July 18, 2023, a coconspirator overseas IT worker associated with Customer-4, posing as U.S. Person-1, and using U.S. Person-1's identification information obtained employment at U.S. Company-7, a staffing company in Pennsylvania.

U.S. Person-2

d. In or around January 2024, a coconspirator overseas IT worker associated with Customer-4, posing as U.S. Person-2, a U.S. citizen, and using U.S. Person-2's identification information applied to an identified U.S. company ("U.S. Company-2"), specifically for a contract position with the U.S. government agency. 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 DIDENKO's Tennessee laptop farm, which was not U.S. Person-2's recorded address. The coconspirator overseas IT worker posing as 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.

e. On or about January 4, 2024, Customer-4 exchanged communications via wires in interstate commerce with DIDENKO, asking "Is Tenneessee [sic] delivery office working now? New laptop will be delivered soon . . . Delivery name will be [U.S. Person-2]".

f. In or around February 2024, a coconspirator overseas IT worker associated with Customer-4, posing as U.S. Person-2, and using U.S. Person-2's identification information applied for employment at an identified U.S. company ("U.S. Company-4"). The coconspirator overseas IT worker provided U.S. Company-4 with a fake driver's license and Social Security card in the name of U.S. Person-2, which U.S. Company-4 determined were falsified documents.

g. In or around March 2024, a coconspirator overseas IT worker associated with Customer-4, posing as U.S. Person-2, and using U.S. Person-2's identification information received a job offer at another identified U.S. company ("U.S. Company-3"). U.S. Company-3 conducted three video interviews of the individual who indicated he was based in Pennsylvania and was willing to relocate. The conspirator overseas IT worker requested a relocation bonus to be deposited directly into his account, but eventually agreed for the prepaid debit card to be sent to the DIDENKO's Tennessee laptop farm.

h. Between on or about January 4, 2024, and on or about March 11, 2024, a coconspirator overseas IT worker associated with Customer-4, posing as U.S. Person-2, and using false documentation purportedly belonging to U.S. Person-2

applied for employment at four additional U.S. Companies (U.S. Company-8, -9, -10, -11).

U.S. Person-3

i. On or about September 22, 2023, Customer-7 exchanged communications via wires in interstate commerce with DIDENKO, "I have shipped one equipment to VA address." Further communications with Customer-7 show this laptop to be associated with a coconspirator overseas IT worker using the identity of U.S. Person-3, a U.S. citizen.

j. Between on or about October 2, 2023, and on or about November 17, 2023, a coconspirator overseas IT worker associated with Customer-7, posing as U.S. Person-2, and using U.S. Person-2's identification information performed contract employment through a staffing company at U.S. Company-13, a luxury retail chain. The coconspirator overseas IT worker provided the staffing company with a fake driver's license and Social Security card in the name of U.S. Person-2.

(**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 Cause the Unlawful Employment of Aliens)

34. The allegations in Paragraphs 1 through 33 of this Indictment are incorporated and re-alleged by reference herein.

35. Between at least in or around 2018, the exact date being unknown to the Grand Jury, and on or about May 10, 2024, DIDENKO 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))

COUNT SEVEN

(Conspiracy to Launder Monetary Instruments)

36. The allegations in Paragraphs 1 through 33 of this Indictment are incorporated and re-alleged by reference herein.

37. Between at least in or around 2018, the exact date being unknown to the Grand Jury, and on or about May 10, 2024, DIDENKO 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 between accounts at U.S. MST-1, U.S. MST-2, Overseas MST-1, and foreign banks, and which involved the proceeds of a specified unlawful activity, that is conspiracy to commit wire fraud as set forth in Count One, conspiracy to commit fraud using identity documents as set forth in Count Five, and prohibition of unlicensed money transmitting business as set forth in Count Nine, 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.

- ***Example of Customers Sending Payments to DIDENKO for Accounts Created***

38. On or about September 24, 2019, Customer-5 exchanged communications via wires in interstate commerce with 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, which is directly linked to his U.S. MST-2 account.

39. On or about September 24, 2019, a coconspirator overseas IT workers sent DIDENKO's U.S. MST-2 account $170 from a U.S. MST-2 account based in China.

40. Between approximately in or around July 2019 and approximately in or around April 2022, Customer-5 used at least three China-based U.S. MST-2 accounts to send DIDENKO's U.S. MST-2 account a total of 148 payments totaling $23,773.

- ***Example of Customers Sending Payments to DIDENKO for "Credit Card" Rental***

41. 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? . . . faktme@gmail.com?" DIDENKO responded, "ok".

42. On or about September 28, 2019, a coconspirator overseas IT worker sent DIDENKO's U.S. MST-2 account $100 from a China-based U.S. MST-2 account.

43. On or about September 28, 2019, DIDENKO's U.S. MST-2 account transferred $100 to a linked account at a Ukraine-based bank, with a payment card ending 1010.

- ***DIDENKO's Movement of Payments for His Scheme Through Various Accounts***

44. Between on or about December 12, 2018, and on or about June 21, 2022, DIDENKO made 677 withdrawal from his U.S. MST-2 account to Ukraine-based bank accounts, totaling $202,422.83.

45. On or about the dates listed below, DIDENKO caused payments from overseas IT workers to be sent to U.S. MST-2 account, and thereafter onto other U.S. MST-2 accounts under different account names, including as follows:

a. On March 3, 2021, a coconspirator overseas IT worker transferred $150 from a Ukraine-based U.S. MST-2 account ("Account-1") to DIDENKO's U.S. MST-2 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, a coconspirator overseas IT worker transferred $1,425 from Account-1 to DIDENKO's U.S. MST-2 account. On the same day, DIDENKO's U.S. MST-2 account transferred $1,425 to Account-2.

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

d. Also on September 27, 2021, a coconspirator overseas IT worker transferred $1,992 from Account-3 to DIDENKO's U.S. MST-2 account. On the same day, DIDENKO's U.S. MST-2 account transferred $1,992 to Account-4.

- ***DIDENKO's Efforts to Avoid Scrutiny from U.S. MSTs***

46. On or about September 6, 2022, a coconspirator customer of DIDENKO's ("Customer-6") exchanged communications via wires in interstate commerce with 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 . . . ."

47. On or about September 6, 2022, a coconspirator overseas IT worker sent a payment of $2,000 to DIDENKO's U.S. MST-2 account, which was finalized on September 8, 2022.

48. On or about May 12, 2023, Customer-4 exchanged communications via wires in interstate commerce with 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".

49. On or about October 25, 2023, Customer-4 exchanged communications via wires in interstate commerce with 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[ount] for that".

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

COUNT EIGHT

(Conspiracy to Launder Monetary Instruments)

48. The allegations in Paragraphs 1 through 47 of this Indictment are incorporated and re-alleged by reference herein.

49. Between at least in or around 2018, the exact date being unknown to the Grand Jury, and on or about May 10, 2024, DIDENKO 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 transport, transmit, or transfer, or attempt to transport, transmit, or transfer monetary instruments and 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 wit, conspiracy to commit wire

fraud as set forth in Count One and conspiracy to commit fraud using identity documents as set forth in Count Five.

(**Conspiracy to Launder Monetary Instruments**, in violation of Title 18, United States Code, Sections 1956(a)(2)(A) & (h))

COUNT NINE

(Prohibition of Unlicensed Money Transmitting Business)

50. The allegations in Paragraphs 1 through 47 of this Indictment are incorporated and re-alleged by reference herein.

51. Between at least in or around 2018, the exact date being unknown to the Grand Jury, and on or about May 10, 2024, DIDENKO and others known and unknown to the Grand Jury, within the District of Columbia and elsewhere, 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)

FORFEITURE ALLEGATION

52. The allegations contained in Counts One through Nine 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).

53. 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, DIDENKO 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 accounts, affiliated with DIDENKO;:

b. Wages and monies accrued by coconspirator overseas IT workers;

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

54. The allegations contained in Counts One through Nine 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).

55. 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, DIDENKO 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 accounts, affiliated with DIDENKO;

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

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

56. 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

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