

UNITED STATES DISTRICT COURT

for the
District of Columbia

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



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:

Table with 2 columns: Code Section and Offense Description. Includes sections like 18 U.S.C. § 371, 1343 & 1349, 1028A, 1028(a)(7), (b)(1)(D),(c)(3) (A) & (f), 1324a & 18 U.S.C. §§ 2, 371, 1956(a)(1)(B)(i) & (h)(a) (2)(A), & (h); and 18 U.S.C. § 1960.

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.

Handwritten signature of David Booth

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 anydesk³ 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

██████████ (“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 ██████████ (“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

- ██████████@gmail.com, and a Ukrainian passport.
- iv. The Ukrainian passports for the ██████████@gmail.com and ██████████@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: ██████████@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 ██████████@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. Financial Transactions

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. It 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 Tennessee [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