UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA

Norfolk Division

IN THE MATTER OF THE SEARCH OF 2353 UPPER GREENS PLACE, VIRGINIA BEACH, VA 23456	Case No.2:24-SW-85 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

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

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search 2353 Upper Greens Place, Virginia Beach, VA 23456 ("**Subject Premises**") The items and evidence to be seized are further described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since 2021 when I completed new agent training at the FBI Academy in Quantico, Virginia. I am presently assigned to the New York Field Office. I have been involved and trained 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.

3. I submit the facts in this affidavit establish probable cause that evidence, fruits, and/or instrumentalities, specifically described in Attachment B, of violations of 18 U.S.C. § 371 (Conspiracy to defraud the United States and its agencies), 18 U.S.C. § 1343 and 1349 (Wire fraud and conspiracy to commit wire fraud), 18 U.S.C. § 1028A (Aggravated identity theft), 18 U.S.C.

§ Section 1028(a)(7), (b)(1)(D), (c)(3)-(A), and (f) (Fraud and related activity in connection with identification documents, authentication features, and information), 8 U.S.C. § 1324a (Unlawful employment of aliens), 18 U.S.C. § 1956(a)(1)(B)(i) and (h)(a)(2)(A), and (h) (Laundering of monetary instruments and conspiracy to commit laundering of monetary instruments), and 18 U.S.C. § 1960 (Unlicensed money transmitting business) (the "target offenses") involving [redacted], OLEKSANDR DIDENKO, and others known and unknown will be found at the **Subject Premises**.

4. The **Subject Premises**, further described in Attachment A, is located in the Eastern District of Virginia.

5. According to the Virginia Department of Motor Vehicles records, [redacted] is a 29-year-old woman ([redacted]) whose address is the **Subject Premises**. According to Department of State and Department of Homeland Security records, [redacted] is a Ukrainian national who entered the United States in June 2022 on Ukrainian Humanitarian Parole.

6. Because this affidavit is being submitted for the limited purpose of establishing probable cause in support of the requested search warrants, I have not included every fact known to me concerning this investigation.

7. The facts in this affidavit are based on my personal knowledge, training, experience, information provided to me by other law enforcement officers, records and other information provided to the FBI, as well as my review of publicly available information.

STATUTES AND BACKGROUND

Relevant Criminal Statutes

8. 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.

9. 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.

10. 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).

11. 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.

12. 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."

13. 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.

14. Under 18 U.S.C. § 1960, it is unlawful to own or operate an "unlicensed money transmitting business," which is defined as "any money transmitting business affecting interstate or foreign commerce…and…otherwise involves the transportation or transmission of funds that are known to the defendant to have been derived from a criminal offense or are intended to be used to promote or support unlawful activity…"

U.S. Government Agencies

15. 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.

16. 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 the 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.

17. The Social Security Administration (SSA) is the federal agency responsible for administering retirement, disability, survivor, and family benefits, and enrolling eligible individuals in Medicare. The 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 the 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 the SSA based on this reported information.

SUMMARY OF THE INVESTIGATION

18. 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

19. 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 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.

---

[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.

20. UpWorkSell is operated by DIDENKO. The UpWorkSell website lists the following "Contact" information: (1) email address [redacted] ("Subject Account-1"); and (2) Telegram handle [redacted]. Subscriber records received for Subject Account 1 listed email address [redacted] ("Subject Account-2") and phone number [redacted] ("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 for an account belonging to DIDENKO at a U.S. MST located in New York ("MST-2") show that Subject Account-2 and Subject Phone Number-1 are listed as the primary methods of contact.

21. 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.[2] In coordination with co-conspirators, DIDENKO facilitates the operation of at least 3 U.S.-based "laptop farms"[3] 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.

---

[2] In this context, proxy means identities of, and accounts created and verified by, real people that someone else uses for their own purposes and to conceal their true identities.

[3] 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.

Services Provided by Didenko

22. DIDENKO provides access to proxy financial accounts in return for payment. These proxy accounts include 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.

23. UpWorkSell's website also offers to create "credit cards" and then rents the use of those cards to its 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.

24. 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.

25. 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).

26. 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.

27. 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.

28. 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"

29. 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 foreigners with accessing and 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 to ensure those IT workers are doing their jobs from the location they claim to be working from. The laptop farm system is used by IT workers so they can credibly claim to be located in the United States and not use a foreign IP address.

30. 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, sets up the computers, and maintains 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:

31. **2353 Upper Greens Place, Virginia Beach, VA 23456 ("Subject Premises")** –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 the address of the **Subject Premises** 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 the **Subject Premises**. Approximately two days later, DIDENKO sent Customer-2 a message, "Hi! Your USA PC is activated." "We can provide anydesk[4] access." "200$ is prepayment."

32. A review of messages from Subject Account-3 shows a discussion between DIDENKO and an unidentified customer ("Customer-9") on or about January 26, 2024 about returning a laptop. Customer-9 informed DIDENKO in a series of messages, "I have to send

[4] 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.

Daniel laptop to the company," "They will change my laptop and will send another laptop," "polina has it." The following day, Customer-9 wrote to DIDENKO, "...please ship to ups and send me the picture of the receipt after deliver to the ups." DIDENKO responded, "ok, give me Label. we will send...," "if you don't have label – we can send ourself," "but in this case you need to pay 100$." Customer replied, "I will pay." After Customer-9 asked, "When can you deliver that and share me picture of receipt" and DIDENKO responded, "I will ping Polina and let you know." On or about January 29, 2024, Customer-9 informed DIDENKO that the laptop had still not been mailed. DIDENKO texted, "Polina worked on Saturday, and post offices are closed on Sunday."

33. FedEx records indicate that the **Subject Premises** received four shipments between September 13, 2023 and December 26, 2023, including two that were labeled as laptop monitors. These two packages were mailed to the **Subject Premises**, but were addressed to the name of an individual (U.S. Person-3, discussed below) who one of DIDENKO's customers was impersonating.

34. On May 6, 2024, law enforcement spoke to an individual who confirmed that [redacted] does live at the **Subject Premises** and is frequently seen in the neighborhood.

35. Additionally, a review of messages from Subject Account-3 revealed that on or about September 19, 2023, DIDENKO messaged one of his customers (Customer-7, discussed below) the address of the **Subject Premises**. The customer asked, "How many laptops are there in VA address?" DIDENKO answered, "9 laptop now."

36. 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.

37. 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.

38. **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.

39. A review of Online Message Provider-1 messages found in Subject Account-3 shows that, in October 2023, DIDENKO received via chat an inquiry from Customer-2 if he/she could have another computer sent to U.S. Co-Conspirator-1's address. DIDENKO responded, "Ofc you can, but let's use another address" and then provided U.S. Address-2 and the name "[redacted]" ("U.S. Co-Conspirator-3"). Approximately five days later, Customer-2 messaged DIDENKO with a tracking number for the shipment. The following day, DIDENKO messaged a confirmation that the laptop had been picked up.

40. 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 a F1 visa.

41. 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.

42. **3067 5th Avenue Apt 202, San Diego, CA 92103 ("U.S. Address-3")** – A Review of messages found in Subject Account-3 shows that, in November 2023, DIDENKO had an exchange with an unidentified customer ("Customer-3") in which Customer-3 wrote, "Hi, I need remote PC connection in US. Company will send PC in US." After DIDENKO responded, "We can help you." Customer-3 asked, "Which state and price?" DIDENKO answered, "[I]n california 400." Customer-3 asked, "[H]ow many PCs is he managing now?" DIDENKO answered, "15 now." Later in the conversation, DIDENKO sent a message to Customer-3 with U.S. Address-3 and the name [redacted]" ("U.S. Co-Conspirator-4"). Approximately two weeks later, Customer-3 messaged DIDENKO a shipping tracking number for a laptop shipment. Approximately two days later, DIDENKO messaged in reply, "The agent informed me 2 minutes ago that we received the package."

43. 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

44. 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."

45. 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."

46. 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.

Examples of The Scheme

47. 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.

48. 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]

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] 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] This email appears in DIDENKO's spreadsheet of proxy identities next to the name of U.S. Person-1.

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

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

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

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

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

iii. Records of U.S. MST-2 show that an account was registered on or about October 28, 2023, with U.S. Person-1's name, email address [redacted] 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 the address for the **Subject Premises** 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 (located in Tennessee) followed by, "New address to new PC's. You can use anyname."

Financial Transactions

49. 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.

50. 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."

51. 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.

52. 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," DIDENKO responded, "we do not recommend sending large amounts together. If would be better to break it up into smaller amounts. Now you need to wait for the transaction to be completed . . . ."

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

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

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

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

Use of Stolen U.S. Person Identities

53. 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

54. 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.

55. 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 masthev75@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.

56. 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."

57. 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

58. 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.

59. 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.

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

61. 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

62. 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.

63. 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.

False Information Transmitted to the U.S. Government

64. 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

65. 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.

Connection to North Korea

Background on North Korea IT Worker Schemes

66. 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

67. 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 **Subject Premises**. 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 **Subject Premises**, 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."

68. 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.

69. 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

70. 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."

71. 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)."

Conclusion

71. Based on the foregoing, your affiant submits that there is probable cause to believe that, from approximately January 2018 until the present, DIDENKO, [redacted] and others known and unknown, have violated, caused to be violated, aided and abetted violations of the target offenses, or conspired to do the same

DIGITAL EVIDENCE STORED WITHIN ELECTRONIC STORAGE MEDIA

72. As described in Attachment B, this application seeks permission to search for records that might be found in or on the **Subject Premises**, in whatever form they are found, including data stored on a computer, cellular phone, tablet, or other media storage device, such as a thumb drive, CD-ROM, DVD, Blu Ray disk, memory card, or SIM card (hereafter collectively referred to as "electronic storage media"). Thus, the warrant applied for would authorize the seizure of all electronic storage media found in or on the **Subject Premises** and, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

73. *Probable cause.* Your Affiant submits that if electronic storage media are found in or on the **Subject Premises**, there is probable cause to believe records and information relevant to the criminal violations set forth in this Affidavit will be stored on such media, for at least the following reasons:

a. Your Affiant knows that when an individual uses certain electronic storage media, the electronic storage media may serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic storage media is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic storage media is also likely to be a storage medium for evidence of crime. From my training and experience, your Affiant believes that electronic storage media used to commit a crime of this type may contain: data that is evidence of how the electronic storage media was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

b. Based on my knowledge, training, and experience, your Affiant knows that electronic storage media contain electronically stored data, including, but not limited to, records related to communications made to or from the electronic storage media, such as the associated telephone numbers or account identifiers, the dates and times of the communications, and the content of stored text messages, e-mails, and other communications; names and telephone numbers stored in electronic "address books;" photographs, videos, and audio files; stored dates, appointments, and other information on personal calendars; notes, documents, or text files; information that has been accessed and downloaded from the Internet; and global positioning system ("GPS") information.

c. Based on my knowledge, training, and experience, your Affiant knows that electronic files or remnants of such files can be recovered months or even years

after they have been downloaded onto an electronic storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on an electronic storage medium, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

d. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the electronic storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

e. As previously set forth in this Affidavit, the targets of this investigation have used computers to execute their fraudulent scheme, including to allow individuals located overseas to log onto U.S. businesses' networks. Therefore, your Affiant believes that evidence of criminal activity will be found on any electronic storage media found at the **Subject Premises** and that the electronic storage media constitute instrumentalities of the criminal activity.

74. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronic files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the electronic storage media were used, the purpose of their use, who used them, and when. There is

probable cause to believe that this forensic electronic evidence will be found on any electronic storage media located in or on the **Subject Premises** because:

a. Data on a storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. File systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within electronic storage medium (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history,

and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the owner. Further, activity on an electronic storage medium can indicate how and when the storage medium was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on an electronic storage medium may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the existence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera) not previously identified. The geographic and timeline information described herein may either inculpate or exculpate the user of the

electronic storage medium. Last, information stored within an electronic storage medium may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information within a computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on an electronic storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic storage medium evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on one electronic storage medium is evidence may depend on other information stored on that or other storage media and the application of knowledge about how electronic storage media behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how an electronic storage medium was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the

presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

75. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a **Subject Premises** for information that might be stored on electronic storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the **Subject Premises**, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on **Subject Premises** could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine electronic storage media to obtain evidence. Electronic storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. *Technical requirements.* Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and

configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the **Subject Premises**. However, taking the electronic storage media off-site and reviewing it in a controlled environment allows for a thorough examination with the proper tools and knowledge.

c. *Variety of forms of electronic media.* Records sought under this warrant could be stored in a variety of electronic storage media formats that may require off-site reviewing with specialized forensic tools.

76. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant your Affiant is applying for would permit seizing, imaging, or otherwise copying electronic storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

BIOMETRIC ACCESS TO DEVICES

77. This warrant permits law enforcement to compel [redacted] at the **Subject Premises** to unlock any devices requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic

devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. Due to the foregoing, if law enforcement personnel encounter any devices that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of [redacted] present at the **Subject Premises** to the fingerprint scanner of the devices found at the **Subject Premises**; (2) hold the devices found at the **Subject Premises** in front of the face of [redacted] present at the **Subject Premises** and activate the facial recognition feature; and/or (3) hold the devices found at the **Subject Premises** in front of the face of [redacted] present at the **Subject Premises** and activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized

by this warrant. The proposed warrant does not authorize law enforcement to compel that [redacted] present at the **Subject Premises** to state or otherwise provide the password or any other means that may be used to unlock or access the devices. Moreover, the proposed warrant does not authorize law enforcement to compel [redacted] present at the **Subject Premises** to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

CONCLUSION

78. Based on the foregoing, I submit that this affidavit supports probable cause for a warrant to search the **Subject Premises** described in Attachment A, and seize the items described in Attachment B.

Respectfully submitted,

David Booth

David Booth
Special Agent
Federal Bureau of Investigation

by telephone - DEM

Subscribed and sworn to before me on May 7, 2024.

The Honorable Douglas E. Miller
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

The Subject Premises to be search is the property described as 2353 Upper Greens Place, Virginia Beach, VA 23456, and includes any outbuilding, shed, storage space, basement, treehouse, garage, or vehicles located on the property. It is further described as a detached two-story house with an attached garage. The exterior is composed mostly of gray brick. The roof is covered in black shingles. A photograph and overview are depicted below:

ATTACHMENT B
Property to Be Seized

1. The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. § 371 (Conspiracy to defraud the United States and its agencies), 18 U.S.C. § 1343 and 1349 (Wire fraud and conspiracy to commit wire fraud), 18 U.S.C. § 1028A (Aggravated identity theft), 18 U.S.C. § Section 1028(a)(7), (b)(1)(D), (c)(3)-(A), and (f) (Fraud and related activity in connection with identification documents, authentication features, and information), 8 U.S.C. § 1324a (Unlawful employment of aliens), 18 U.S.C. § 1956(a)(1)(B)(i) and (h)(a)(2)(A), and (h) (Laundering of monetary instruments and conspiracy to commit laundering of monetary instruments), and 18 U.S.C. § 1960 (Unlicensed money transmitting business) occurring in or after July 2018, including:

a. records and information relating to a conspiracy to defraud entities seeking to employ remote workers;

b. records and information relating to a conspiracy to launder funds;

c. employment records;

d. financial records;

e. personal identification documents for [redacted]

f. records and information relating to the location of participants in a scheme to defraud U.S.-based entities seeking to employ remote workers;

g. records and information related to individuals gaining employment as a remote worker;

h. records and information related to U.S.-based entities who employed remote workers;

i. records and information relating to the identity or location of the suspects;

2. Books, records, receipts, notes, ledgers, invoices, and any other documentation related to the scheme;

3. Notes containing the individual names of such persons, telephone numbers or addresses of associates in the schemes, and any records of accounts receivable, money paid or received, cash or checks received, or intended to be paid;

4. Packaging and shipping materials;

5. Records relating to the receipt, transportation, deposit, transfer, or distribution of money, including but not limited to, direct deposit confirmations, wire transfers, money orders, cashier's checks, check stubs, PayPal, Payoneer, or other electronic money transfer services, check or money order purchase receipts, account statements, and any other records reflecting the receipt, deposit, or transfer of money;

6. United States currency, foreign currency, financial instruments, negotiable instruments, jewelry, precious metals, stocks, bonds, money wrappers, and receipts or documents regarding purchases of real or personal property;

7. Safe deposit box keys, storage locker keys, safes, and related secure storage devices, and documents relating to the rental or ownership of such units;

8. Indicia of occupancy, residency, rental, ownership, or use of the Subject Premises and any vehicles found thereon during the execution of the warrant, including, utility and telephone bills, canceled envelopes, rental, purchase or lease agreements, identification documents, keys, records of real estate transactions, vehicle titles and registration, and vehicle maintenance records;

9. Photographs, including still photos, negatives, slides, videotapes, and films, in particular those showing co-conspirators, criminal associates, U.S. currency, real and personal property;

10. Computers, cellular phones, tablets, and other media storage devices, such as thumb drives, CD-ROMs, DVDs, Blu Ray disks, memory cards, and SIM cards (hereafter referred to collectively as "electronic storage media");

11. Records evidencing ownership or use of electronic storage media, including sales receipts, registration records, and records of payment;

12. Any records and information found within the digital contents of any electronic storage media seized from the Subject Premises, including:

a. all information related to the offenses as described in paragraph 1;

b. all bank records, checks, credit card bills, account information, or other financial records;

c. any information recording schedule or travel;

d. evidence of who used, owned, or controlled the electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, correspondence, and phonebooks;

e. evidence indicating how and when the electronic storage media were accessed or used to determine the chronological context of electronic storage media access, use, and events relating to crime under investigation and to the electronic storage media user;

f. evidence indicating the electronic storage media user's state of mind as it relates to the crime under investigation;

g. evidence of the attachment to an electronic storage medium of another storage device or similar container for electronic evidence;

h. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the electronic storage media;

i. evidence of the times the electronic storage media were used;

j. passwords, encryption keys, and other access devices that may be necessary to access the electronic storage media;

k. documentation and manuals that may be necessary to access the electronic storage media or to conduct a forensic examination of the electronic storage media;

l. records of or information about Internet Protocol addresses used by the electronic storage media;

m. records of or information about the electronic storage media's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses;

n. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as prints, slides, negatives, videotapes, motion

pictures, or photocopies). This shall include records of telephone calls; names, telephone numbers, usernames, or other identifiers saved in address books, contacts lists and other directories; text messages and other stored communications; subscriber and device information; voicemails or other audio recordings; videos; photographs; e-mails; internet browsing history; calendars; to-do lists; contact information; mapping and GPS information; data from "apps," including stored communications; reminders, alerts and notes; and any other information in the stored memory or accessed by the electronic features of the computer, electronic device, or other storage medium.

Use of Biometric Features. During the execution of this search warrant, law enforcement is permitted to: (1) depress [redacted] thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of [redacted] faces with their eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in *Graham v. Connor*, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

Further, law enforcement may compel the use of the biometric features described above if: (1) the procedure is carried out with dispatch and in the immediate vicinity of the premises to be searched; and (2) at the time of compulsion, the government has reasonable suspicion that the suspect has committed a criminal act that is the subject matter of the warrant and that the individual's biometric features will unlock the device.

This warrant authorizes a review of records and information seized, copied or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this

warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.