AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

District of Oregon

SEALED

United States of America
v.
SALWAN ADJAJ

Case No. 3:21-mj-201

Defendant(s)

CRIMINAL COMPLAINT
BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

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 February through May 2021 in the county of Clackamas in the _____ District of Oregon, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 1028A	Aggravated Identity Theft
18 U.S.C. § 1343	Wire Fraud

This criminal complaint is based on these facts:

See the attached affidavit, whihc is incorporated herein by reference.

☒ Continued on the attached sheet.

Complainant's signature

Andrew P. Smith, Special Agent, TIGTA

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone at 11:05 ~~x~~ a.m./p.m.

Date: October 14, 2021

Youlee Yim You

Judge's signature

City and state: Portland, Oregon Hon. Youlee Yim You, U.S. Magistrate Judge

Printed name and title

3:21-mj-201

SEALED

DISTRICT OF OREGON, ss: AFFIDAVIT OF ANDREW P. SMITH

Affidavit in Support of a Criminal Complaint and Arrest Warrant

I, Andrew P. Smith, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent of the Treasury Inspector General for Tax Administration ("TIGTA") and have been so employed since March 2020. I am currently assigned to the Seattle Group, Western Field Division, office in Portland, Oregon. I have received basic federal law enforcement training, including at the United States Army Criminal Investigation Division Special Agent Course, as well as other specialized federal law enforcement training. I have investigated violations of federal statutes, including wire fraud, bank fraud, mail fraud, identity theft, extortion, false personation, conspiracy, and theft of government and public money. I have been a sworn federal law enforcement officer during all times covered herein.

2. I submit this affidavit in support of a Criminal Complaint and arrest warrant for SALWAN ADJAJ ("ADJAJ"), a United States citizen, for wire fraud and aggravated identity theft in violation of Title 18, United States Code, sections 1343 and 1028A, respectively. As set forth below, there is probable cause to believe, and I do believe, that ADJAJ committed said offenses by submitting or causing to be submitted fraudulent applications for loans issued or guaranteed by the United States Small Business Administration ("SBA") from and in the District of Oregon between February 2021 and June 2021.

3. I also submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises located at 31190 SW Isle Way, Lane West Linn, OR 97068 (hereinafter OR ADDRESS 1) and the person of SALWAN ADJAJ.

4. The information set forth in this affidavit consists of information I have gathered and information relayed to me by other law enforcement personnel and civilian witnesses and by my own review and analysis of various official and financial records. The information in this affidavit is not intended to detail each and every fact and circumstance of the investigation or all information known to me or other participants in the investigation. Rather, this affidavit serves solely to establish that probable cause exists in support of the offenses charged in this complaint and to establish that there is probable cause to conclude that evidence and fruits of those offenses will be found at the Premises.

Applicable Law

5. Title 18 U.S.C. § 1028A, specifies, in relevant part: "Whoever, during and in relation to any felony violation enumerated in subsection (c) [including violations of 18 U.S.C. § 1343], knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years."

6. Title 18, U.S.C. § 1343, specifies, in relevant part: "Whoever, having devised 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, shall be fined under this title or imprisoned not more than 20 years, or both."

Statement of Probable Cause

The Economic Injury Disaster Program

7. The Economic Injury Disaster Loan ("EIDL") program is an SBA program providing low-interest financing to small businesses, renters, and homeowners affected by declared disasters. The Coronavirus Aid, Relief, and Economic Security Act ("CARES Act") and Coronavirus Response and Relief Supplemental Appropriations Act ("CRRSAA") authorized the SBA to issue EIDLs (and advances of up to $10,000) to small businesses adversely affected by the Coronavirus pandemic and associated mitigation measures. EIDLs are determined by the number of certified employees on the applicant's payroll and must be repaid. Advances do not have to be repaid.

8. To obtain an EIDL or EIDL advance, qualifying businesses must submit an application to the SBA and provide information about business operations, such as the number of employees, gross revenues for the 12-month period preceding the disaster, and cost of goods sold in the 12-month period preceding the disaster; in the case of EIDLs for COVID-19 relief, the relevant 12-month period is the year preceding January 31, 2020. The applicant must also certify all application information submitted is true and correct to the best of the applicant's knowledge.

9. EIDL applications are submitted electronically to the SBA through servers in Colorado and processed by the agency with support from Rapid Finance, a government contractor managing the EIDL program. The amount of an EIDL, if approved, is determined based, in part, on information provided by the applicant about employment, revenue, and cost of goods, as described above. Any funds disbursed as an EIDL or advance are issued directly by the SBA. EIDL funds can be used for payroll expenses, sick leave, production costs, and

business obligations, such as debts, rent, and mortgage payments. If the applicant also obtains a Paycheck Protection Program ("PPP") loan, the EIDL funds cannot be used for the same purpose as the PPP funds.

10. The SBA, Office of Inspector General (OIG), is supporting this investigation and has direct access to EIDL data, which may be used for the purpose of investigations relating to abuses of the EIDL Program and any resulting criminal, civil, or administrative proceedings.

The Restaurant Revitalization Fund

11. On March 11, 2021, the President signed the American Rescue Plan Act ("ARPA"). Section 5003 of ARPA established the Restaurant Revitalization Fund ("RRF") and appropriated $28.6 billion to the SBA for the purpose of making grants under that program. The SBA awards funding through the RRF to restaurants, bars, and similar businesses serving food or drink. The purpose of this funding is to provide support to eligible entities that suffered revenue losses as a result of the COVID-19 pandemic and related mitigation measures.

12. The RRF includes specific requirements to ensure equitable distribution to small business concerns owned by women, veterans, and socially and economically disadvantaged Applicants.

13. The RRF application is to be completed by applicants applying for funding under the RRF. The SBA collects the requested information to determine whether applicants are eligible for funding. Instructions and definitions are located at the end of each application.

14. The SBA may provide funding of up to $5,000,000 per location (not to exceed $10,000,000 total for the Applicant and any affiliated businesses) for Applicants who meet certain conditions. The minimum award was set at $1,000; therefore, applications for less than $1,000 were not accepted. Awardees are not required to repay funds received under the

Restaurant Revitalization Program unless funds are used for purposes that are not specifically authorized, are not used by March 11, 2023, or the recipient permanently closed before using all funds on authorized purposes.

15. The SBA Office of Inspector General (OIG) has direct access to RRF data, which may be used for the purpose of investigations relating to abuses of the RRF program and any resulting criminal, civil, or administrative proceedings.

ADJAJ's Attempts to Defraud the EIDL Program in March 2021

16. SALWAN ADJAJ DMD PC ("SUBJECT BUSINESS 1") is an Oregon company. ADJAJ is the company's president.

17. Heart and Soil Farm ("SUBJECT BUSINESS 2") was assigned an EIN by the IRS on or about March 1, 2021. ADJAJ was the applicant for the EIN associated with SUBJECT BUSINESS 2 and was its general partner. It is located in Clackamas County, Oregon. The mailing address for SUBJECT BUSINESS 2 is OR ADDRESS 1.

18. Rose City ("SUBJECT BUSINESS 3") was assigned an EIN by the IRS on or about March 12, 2021. ADJAJ was the applicant for the EIN associated with SUBJECT BUSINESS 3 and was its general partner. SUBJECT BUSINESS 3 is located at 11689 NE Glisan Street, Portland, Oregon ("OR ADDRESS 2"). The mailing address for SUBJECT BUSINESS 3 is OR ADDRESS 1.

19. MARWAN ADJAJ ("SUBJECT BUSINESS 4") was assigned an EIN by the IRS in or around March 2021, and is located at 1521 SW Coast Avenue, Lincoln City, Oregon ("OR ADDRESS 3"). The mailing address for SUBJECT BUSINESS 4 is OR ADDRESS 1.

20. MARWAN ADJAJ DMD PC ("SUBJECT BUSINESS 5") was assigned an EIN by the IRS on or about March 8, 2021. VICTIM 1, an actual person, was the purported applicant for the EIN associated with SUBJECT BUSINESS 5, which is located at 20015 SW Pacific Highway, Suite 220, Sherwood, Oregon ("OR ADDRESS 4"). The mailing address for SUBJECT BUSINESS 5 is OR ADDRESS 1.

21. TASHA HODGES ("SUBJECT BUSINESS 6") was assigned an EIN by the IRS on or about March 2, 2021. VICTIM 2, an actual person, was the purported applicant for the EIN associated with SUBJECT BUSINESS 6, which is located at OR ADDRESS 3. The mailing address for SUBJECT BUSINESS 6 is OR ADDRESS 1.

22. As described further below, evidence gathered in the investigation demonstrates that, in or around March 2021, ADJAJ submitted, or caused to be submitted, fraudulent loan applications to the SBA in order to obtain funds through the EIDL program. Among other things, ADJAJ knowingly provided false information concerning the business start dates, numbers of employees, and identities of the purported applicants and businesses owners.

23. Specifically, ADJAJ submitted, or caused to be submitted, the following fraudulent EIDL applications—among dozens of others—on behalf of the following subject businesses (collectively referred to as "the EIDL APPLICANTS"):

///

///

///

///

///

///

Applicant:	Application Number:	Date of Application:	Result:
SUBJECT BUSINESS 2	3317489290	3/1/2021	Declined
SUBJECT BUSINESS 3	3317732948	3/12/2021	Declined
SUBJECT BUSINESS 4	3317722534	3/11/2021	Declined
SUBJECT BUSINESS 5	3317649278	3/8/2021	Declined
SUBJECT BUSINESS 6	3317500559	3/1/2021	Declined

Evidence of Fraud in the EIDL Applications

24. A comparison of the representations in the above-listed EIDL applications with government records associated with the EIDL APPLICANTS revealed several apparent falsehoods in those applications.

a. All of the EIDL APPLICANTS were purported to employ multiple people, but the IRS did not have any record of any of the EIDL APPLICANTS' ever having filed any annual or quarterly employment tax returns.

b. All of the EIDL APPLICANTS purportedly started business operations before January 31, 2020, but IRS records reflected that the EINs for all of the EIDL APPLICANTS were assigned in or around March 2021. Additionally, despite the fact that all of the EIDL APPLICANTS were purportedly based in Oregon, only SUBJECT BUSINESS 4 had ever registered with Oregon's Secretary of State—and that registration did not occur until March 2021.

25. All of the above-listed EIDL applications were also closely associated with ADJAJ, despite the fact that most of them were submitted in other persons' names.

a. According to IRS records, all of the EIDL APPLICANTS used OR ADDRESS 1 as their mailing address, and that address is ADJAJ's personal residence.

b. All of the EIDL APPLICANTS directed the proceeds of the requested EIDLS to a Bank of America account ending in 3034 ("SUBJECT ACCOUNT 1"). Bank of America's records indicate SUBJECT ACCOUNT 1 was owned and controlled by ADJAJ's own dental practice (SUBJECT BUSINESS 1) and ADJAJ.

c. All of the EIDL APPLICANTS claimed the same telephone number: (503) 969-8471 ("SUBJECT PHONE 1"). Numerous records identify SUBJECT PHONE 1 as belonging to ADJAJ.

d. All of the above-listed EIDL applications were submitted from Internet Protocol (IP) address 71.237.252.127, associated with a physical location in Happy Valley, Oregon ("IP ADDRESS 1"). The associated Internet Service Provider's records from May 2021 (older records are unavailable) indicate that IP ADDRESS 1 was registered to ADJAJ's own dental practice (SUBJECT BUSINESS 1), with ADJAJ's personal residence (OR ADDRESS 1) as the listed billing address.

26. Based on the above-described apparent falsehoods and common use of ADJAJ's residential address, IP address, bank account, and telephone number in the applications submitted on behalf of the EIDL APPLICANTS, I believe ADJAJ submitted numerous false and fraudulent EIDL applications to SBA using interstate wires in violation of 18 U.S.C. § 1343. I also believe ADJAJ used identifying information, specifically the names, of at least two other actual persons without lawful authority in the submission of these fraudulent applications in violation of 18 U.S.C. § 1028A.

ADJAJ's Involvement in Defrauding the RRF Program

27. SBA records indicate the ADJAJ shifted his sights to the RRF program by May 2021 and met with substantially greater success.

28. HEATHER PERKINS ("SUBJECT BUSINESS 7") was assigned an EIN by the IRS in or around March 2021, and is located at 5618 New York Avenue, Sarasota, Florida ("FL ADDRESS 1"). The mailing address for SUBJECT BUSINESS 7 is OR ADDRESS 1.

29. DAYAMI MUNOZ ("SUBJECT BUSINESS 8") was assigned an EIN by the IRS on or around March 30, 2021. VICTIM 3, an actual person, was the purported applicant for the EIN associated with SUBJECT BUSINESS 8, which is located at 7355 NW 5th Street, Miami, Florida ("FL ADDRESS 2"). The mailing address for SUBJECT BUSINESS 8 is OR ADDRESS 1.

30. AMY WILLIAMS ("SUBJECT BUSINESS 9") was assigned an EIN by the IRS on April 8, 2021. VICTIM 4, an actual person, was the applicant for the EIN associated with SUBJECT BUSINESS 9, which is located at 208 Bellevue Avenue, Daytona Beach, Florida ("FL ADDRESS 3"). The mailing address for SUBJECT BUSINESS 9 is OR ADDRESS 1.

31. Government records and documentary evidence indicate there is probable cause to conclude that ADJAJ submitted or caused to be submitted the following fraudulent RRF loan applications (among others) on behalf of the following subject businesses (collectively "the RRF APPLICANTS"), generating nearly $8 million in fraudulent proceeds:

///

///

///

Applicant:	Application Number:	Date of Application:	Result:	Loan Amount:
SUBJECT BUSINESS 7	30252146	5/11/2021	Funded	$1,685,677.00
SUBJECT BUSINESS 8	30583304	5/13/2021	Funded	$2,660,198.00
SUBJECT BUSINESS 9	30568340	5/13/2021	Funded	$3,463,030.00

32. Each of the above-listed RRF applications was purportedly submitted by a different individual, all residents of Florida, but the evidence suggests they were actually submitted by ADJAJ without the knowledge or authorization of those individuals.

33. A comparison of the representations in the above-listed RRF loan applications with government records associated with the RRF APPLICANTS revealed several apparent falsehoods in those applications.

a. All of the RRF APPLICANTS reported various gross revenues purportedly derived from their Tax Year 2019 and 2020 federal tax returns, but IRS records reflected that the only tax returns ever filed by the RRF APPLICANTS were their 2020 corporate tax returns. Consequently, all of the statements in the RRF loan applications about gross revenues reported on 2019 federal tax returns were false.

b. All of the RRF APPLICANTS claimed that they first began making sales on July 1, 2006, but IRS records reveal that none of the RRF APPLICANTS was assigned an EIN before March 2021. Additionally, although all the RRF APPLICANTS were associated with Oregon and Florida addresses, none of the RRF APPLICANTS had ever registered with either the Oregon Secretary of State or the Florida Secretary of State.

34. Although all the above-listed RRF loan applications were purportedly submitted on behalf of the RRF APPLICANTS by other individuals, records reviewed during the course of the investigation tie ADJAJ to the applications.

c. According to records from the IRS, AJAJ's personal residence (OR ADDRESS 1) was the listed mailing address for all the RRF APPLICANTS.

d. The RRF loan application on behalf of SUBJECT BUSINESS 9 directed disbursement of the loan proceeds to a Wells Fargo account ending in 6801 ("SUBJECT ACCOUNT 2"). Wells Fargo bank records establish that SUBJECT ACCOUNT 2 was owned and controlled by ADJAJ's own dental practice (SUBJECT BUSINESS 1) and ADJAJ.

e. The RRF loan application on behalf of SUBJECT BUSINESS 8 directed disbursement of the loan proceeds to a JP Morgan Chase account ending in 6295 ("SUBJECT ACCOUNT 3"). SBA records indicate that ADJAJ himself used SUBJECT ACCOUNT 3 in association with an EIDL application for his own dental practice (SUBJECT BUSINESS 1).

f. All of the RRF APPLICANTS submitted their RRF loan applications from IP ADDRESS 1, which, as described above, is associated with ADJAJ's own dental practice and residential mailing address.

35. Based on the apparent falsehoods in the above-listed RRF loan applications and common use of ADJAJ's residential address, IP address, and bank accounts by the RRF APPLICANTS, I believe ADJAJ submitted numerous false and fraudulent RRF loan applications to SBA using interstate wires in violation of 18 U.S.C. § 1343. I also believe ADJAJ used

identifying information, specifically the names, of at least three other actual persons without lawful authority in the submission of these fraudulent applications in violation of 18 U.S.C. § 1028A.

Search of Premises at OR ADDRESS 1

36. This affidavit is also submitted in support of an application for a warrant to search the premises of OR ADDRESS 1 and the persons and vehicles on those premises. Based on the foregoing facts tying ADJAJ and his commission of wire fraud and aggravated identity theft offenses to that residential address, and based on the fact that, in my training and experience, individuals perpetrating document-intensive financial frauds and identity-theft schemes tend to keep evidence of those offenses and the disposition of the proceeds thereof on their persons, in their vehicles, and in their personal residences, I believe evidence, instrumentalities, and fruits of the above-described offenses will be found at OR ADDRESS 1.

37. As described above and in Attachment B, this application seeks permission to search for certain documents and records that might be found on the premises of OR ADDRESS 1. Some anticipated forms of that evidence include, but are not limited to, personally identifiable information of other individuals in the form of driver's licenses, social security number cards, bank and financial statements, ATM cards, bank cards, gift cards, ATM receipts, cash, mailbox keys, electronic devices, and other digital devices, including digital currency wallets.

Search Process for Digital Devices

38. Evidence and fruits of the above-described offenses will likely be found in data stored on computer hard drives or other storage media and on other digital devices, including cell phones (hereinafter collectively referred to as digital devices), because the fraudulent loan

applications at issue were submitted electronically from IP ADDRESS 1, which is associated with OR ADDRESS 1. Thus, the warrant applied for would authorize the seizure and search of digital devices or the copying of electronically stored information under Rule 41(e)(2)(B).

a. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a digital device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device 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. When a person "deletes" a file on a digital device, the data contained in the file does not actually disappear; rather, that data remains on the digital device until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a digital device's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Wholly apart from user-generated files, digital devices—in particular, internal hard drives—contain electronic evidence of how a digital device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Digital device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

d. Based on actual inspection of other evidence related to this investigation, banking information, reports prepared by the investigative team, and records obtained from the SBA, I am aware that digital devices were used to generate, store, and print documents used in the wire fraud and bank fraud scheme. Thus, there is reason to believe that there is a digital device currently located on the OR ADDRESS 1.

39. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant but also for forensic electronic evidence that establishes how digital devices 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 on any digital device in the OR ADDRESS 1, because, based on my knowledge, training, and experience, I know:

a. Data on the digital device can provide evidence of a file that was once on the digital device 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, email programs, and chat programs store configuration information on the digital device that can reveal information such as online nicknames and passwords. 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 digital device was

in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a digital device can also indicate who has used or controlled it. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time. Further, forensic evidence on a digital device can show how and when it was accessed or used. Such "timeline" information allows the forensic analyst and investigators to understand the chronological context of access to the digital device, its use, and events relating to the offense under investigation. This "timeline" information may tend to either inculpate or exculpate the user of the digital device. Last, forensic evidence on a digital device may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information on a digital device may indicate the user's motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a "wiping program" to destroy evidence on the digital device or password protecting or encrypting such evidence in an effort to conceal it from law enforcement), or knowledge that certain information is stored on a digital device (e.g., logs indicating that the incriminating information was accessed with a particular program).

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how digital devices 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 a digital device 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 evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a digital device is evidence may depend on other information stored on the digital device and the application of knowledge about how a digital device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device 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 digital device. 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.

f. I know that when an individual uses a digital device to commit a crime the individual's digital device will generally serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of crime.

From my training and experience, I believe that a digital device used to commit a crime of this type may contain: data that is evidence of how the digital device 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.

40. In most cases, a thorough search of the OR ADDRESS 1 for information that might be stored on a digital device often requires the seizure of the device and a later, off-site review consistent with the warrant. In lieu of removing a digital device from OR ADDRESS 1, it may be possible to image or copy it. Generally speaking, imaging is the taking of a complete electronic picture of the digital device'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 digital device and to prevent the loss of the data either from accidental or intentional destruction. This is true because:

a. 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 digital device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on 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 digital devices to obtain evidence. Digital devices 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. Records sought under this warrant could be stored in a variety of formats that may require off-site reviewing with specialized forensic tools. Similarly, digital devices 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 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 OR ADDRESS 1. However, taking the digital device off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

41. In my training and experience, it is likely that the OR ADDRESS 1 will contain at least one Apple brand device, such as an iPhone or iPad, because through the course of this investigation we have encountered device identifiers associated with digital devices manufactured by Apple, Inc. A verification of the use of Apple devices was confirmed through a messaging application, which showed the recipient as an Apple iMessage device and application.

42. I know from my training and experience, as well as from information found in publicly available materials including those published by Apple, that some models of Apple devices such as iPhones and iPads offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, "fingerprint") in lieu of a numeric or alphanumeric passcode or password. This feature is called Touch ID.

43. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID

sensor, which is found in the round button (often referred to as the "home" button) found at the bottom center of the front of the device. In my training and experience, users of Apple devices that offer Touch ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

44. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode or password must be used instead. These circumstances include: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; and (3) five unsuccessful attempts to unlock the device via Touch ID are made.

45. The passcode or password that would unlock any Apple device found during the search of the OR ADDRESS 1 is not known to law enforcement. Thus, it will likely be necessary to press the fingers of the users of any Apple device found during the search of the OR ADDRESS 1 to that device's Touch ID sensor in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant Apple device(s) via Touch ID with the use of the fingerprints of the users is necessary because the

government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

46. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via Touch ID, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a OR ADDRESS 1 without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any occupant of OR ADDRESS 1 to press their fingers against the Touch ID sensor of a locked Apple device found during the search of OR ADDRESS 1 in order to attempt to identify the device's user(s) and unlock the device via Touch ID. Based on these facts and my training and experience, it is likely that ADJAJ is one user/are users of the device(s) and thus that his fingerprints are among those that are able to unlock the device via Touch ID.

47. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a Touch ID-enabled Apple device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock a device found in OR ADDRESS 1 as described above within the five attempts permitted by Touch ID, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

48. I therefore request that the Court authorize law enforcement to press the fingers, including thumbs, of individuals found at the OR ADDRESS 1 to the Touch ID sensor of any Apple devices, such as iPhones or iPads, found at the OR ADDRESS 1 for the purpose of attempting to unlock the devices via Touch ID in order to search the contents as authorized by this warrant.

49. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant for which I apply would permit seizing, imaging, or otherwise copying digital devices that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the device or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire device, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

50. The initial examination of the digital device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

51. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the digital device do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without

authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

52. If an examination is conducted, and the digital device does not contain any data falling within the ambit of the warrant, the government will return the digital device to its owner within a reasonable period of time following the search and will seal any image of the digital device, absent further authorization from the Court.

53. The government may retain the digital device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the digital device and/or the data contained therein.

54. The government will retain a forensic image of the digital device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

Conclusion

55. Based on the foregoing, I have probable cause to believe, and I do believe, that SALWAN ADJAJ committed wire fraud and aggravated identity theft in violation of 18 U.S.C. §§ 1343 and 1028A, respectively. I therefore request that the Court issue a criminal complaint

and arrest warrant for SALWAN ADJAJ and a warrant to search the premises of his personal residence, OR ADDRESS 1.

56. Prior to being submitted to the Court, this affidavit and the accompanying Criminal Complaint, arrest warrant, search warrant application, and search warrant were all reviewed by Assistant United States Attorney Ryan W. Bounds, who advised me that in his opinion the affidavit is legally and factually sufficient to establish probable cause to support the issuance of the requested Criminal Complaint and warrants for both ADJAJ's arrest and the search of his residence.

Request for Sealing

57. It is respectfully requested that the Court issue an order sealing, until further order of the Court, all papers submitted in support of the requested criminal complaint, arrest warrant, and search warrant. I believe that sealing these documents is necessary because the information to be seized is relevant to an ongoing investigation, and any premature disclosure of the information at this time may cause flight from prosecution, destruction of or tampering with evidence, or other serious jeopardy to this investigation, undermining the integrity thereof.

_____
ANDREW P. SMITH
Special Agent, TIGTA

Sworn in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone at 11:05 ~~a.m.~~/p.m. on October 14, 2021.

Youlee Yim You
_____
HON. YOULEE YIM YOU
United States Magistrate Judge