AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America

v.

ANDRANIK AMIRYAN,

Defendant(s)

Case No. 2:20-mj-04545-Duty

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.

As described in the accompanying attachment, defendant violated the following statutes:

Code Sections	*Offense Description*
18 U.S.C. §§ 1344, 1349, 1028A 8 U.S.C. § 1326(a), (b)(1)	Conspiracy to Commit Bank Fraud, Aggravated Identity Theft, Illegal Alien Found After Removal

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s Alfredo Rossi
Complainant's signature

Alfredo Rossi, Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: September 23, 2020

Judge's signature

City and state: Los Angeles, California

Hon. Michael Wilner, U.S. Magistrate Judge
Printed name and title

Complaint Attachment

Count One, 8 U.S.C. § 1326(a),(b)(1)

On or about February 28, 2017, defendant ANDRANIK AMIRYAN, an alien, who had been officially deported and removed from the United States on or about April 16, 2008, and January 20, 2011, was found in Los Angeles County, within the Central District of California, after knowingly and voluntarily re-entering and remaining in the United States without having obtained permission from the Attorney General or his designated successor, the Secretary for Homeland Security, to reapply for admission to the United States following deportation and removal.

Defendant's previously alleged removals from the United States occurred subsequent to defendant's conviction for at least one of the following felonies: Burglary, in violation of California Penal Code Section 459, and Get Credit/Goods in Another's Identity, in violation California Penal Code Section 530.5, on or about January 30, 2007, for which defendant was sentenced to two years in prison; Grand Theft, in violation of California Penal Code Section 487, and False Personation Of Another, in violation of California Penal Code Section 529, on or about January 30, 2007, for which defendant was sentenced to three years in prison; and Illegal Alien Found After Removal and Conviction, in violation of 8 U.S.C. § 1326, for which defendant was sentenced to 14 months in prison.

Count Two, 18 U.S.C. § 1349

Beginning on an unknown date, and continuing through at least September 23, 2020, in Los Angeles County, within the Central District of California, and elsewhere, defendant ANDRANIK AMIRYAN, and others, conspired to commit bank fraud, in violation of Title 18, United States Code, Section 1344. The object of the conspiracy was carried out, and to be carried out, in substance, as follows: Defendant would impersonate a victim of identity theft and open bank accounts in the victim's name. Defendant and his co-conspirators would use a shell company to apply for CARES Act relief funds, falsely stating that the shell company had a monthly payroll over $500,000, and attaching forged tax forms as support. Defendant and his co-conspirators would rapidly withdraw the CARES Act funds by writing checks to co-conspirators and to additional shell companies for which defendant had obtained bank accounts. Defendant would also use his bank accounts to accept fraudulently obtained CARES Act relief funds from shell companies controlled by his co-conspirators. As a result of this fraud, defendant and his co-conspirators obtained from federally-insured financial institutions over $1 million by making false statements to the banks.

Count Three, 18 U.S.C. § 1028A

Beginning on an unknown date, and continuing through at least September 23, 2020, in Los Angeles County, within the Central District of California, and elsewhere, defendant ANDRANIK AMIRYAN knowingly transferred, possessed, and used, without lawful authority, a means of identification of another person during and in relation to a felony violation of Title 18, United States Code, Section 1349, Conspiracy to Commit Bank Fraud, as charged in Count Two, knowing that the means of identification belonged to another actual person.

AFFIDAVIT

I, Alfredo Rossi, being duly sworn, declare and state as follows:

I. APPLICATION FOR SEARCH AND ARREST WARRANTS

1. This affidavit is made in support of a warrant to search the residence of ANDRANIK AMIRYAN for evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1343, 1344, 1349, 1028A, and 1956, Wire Fraud, Bank Fraud, Conspiracy, Aggravated Identity Theft, and Money Laundering (the "SUBJECT OFFENSES"), as described more fully in Attachment B, which is incorporated by reference. The residence to be searched, described more fully in Attachment A, which is also incorporated by reference, is:

a. 8442 OSWEGO STREET, SUNLAND, CALIFORNIA ("AMIRYAN'S RESIDENCE").

2. This affidavit is also made in support of a complaint against, and arrest warrant for, ANDRANIK AMIRYAN violations of Title 18, United States Code, Sections 1344, 1349, and 1028A, Conspiracy to Commit Bank Fraud and Aggravated Identity Theft, and Title 8, United States Code, Section 1326(a), (b)(1), Illegal Alien Found After Deportation and Felony Conviction.

II. BACKGROUND OF SPECIAL AGENT ALFREDO ROSSI

3. I am a Special Agent with Homeland Security Investigations ("HSI") and have been so employed since June 2019. I am currently assigned to the High Intensity Financial Crimes Area ("HIFCA") group, where I investigate matters concerning bank fraud, wire fraud, identity theft, money laundering, and other illegal financial transactions.

4. Prior to becoming a Special Agent with HSI, I was employed as Special Agent with the United States Secret Service ("USSS") from June 2016 until June 2019, where I was responsible for the investigation of various types of theft and fraud, including the manufacturing of counterfeit and fraudulent identification documents, and the investigation of financial crimes (such as access device crimes, credit card fraud, check fraud, and schemes to conceal and launder the proceeds of such crimes).

5. To become an HSI Special Agent, I completed 9 months of training at the Federal Law Enforcement Training Center in Brunswick, Georgia. During my employment as an HSI and USSS Special Agent, I have participated in several investigations related to alien smuggling, narcotics smuggling, weapons trafficking, organized criminal activity, child exploitation, and financial crimes. I have participated in various aspects of criminal investigations, including bank records analysis, telephone records analysis, electronic surveillance, physical surveillance, search warrants, arrests, and reviewing evidence from digital devices. I have also spoken to many law enforcement agents regarding their experience in criminal investigations, interviewed defendants, confidential informants, and witnesses who had personal knowledge regarding the methods used to commit various types of criminal offenses.

6. Any facts or circumstances that are cited in this affidavit are familiar to me through my direct participation in this investigation, discussions with other law enforcement personnel involved in this investigation, and/or my review of investigative reports generated by other law enforcement personnel. This affidavit is made for the sole purpose of demonstrating probable cause for the

issuance of the requested search warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. SUMMARY OF PROBABLE CAUSE

7. In or about August 2020, HSI initiated an investigation on ACBA Technologies, Inc. ("ACBA") for having used a stolen identity to receive approximately $650,600 in funds with the Small Business Administration (SBA) through the Paycheck Protection Program ("PPP") and Economic Injury Disaster Loan ("EIDL") established by the Coronavirus Aid, Relief, and Economic Security Act. In or about June 2020, ACBA received PPP funds through First Home Bank ("FHB") and EIDL funds directly from the SBA, which were all disbursed into a Bank of America ("BofA") business account opened in the name of ACBA. Once the money was wired in, at least twenty checks were drawn on the BofA account made payable to a mix of business names and individual names in a manner consistent with money laundering. The ACBA accounts were opened through identity theft and the individual controlling these accounts is AMIRYAN. Some of the owners of the business accounts that received fraudulent funds from ACBA had also fraudulently applied for and obtained additional COVID-19 related relief assistance.

8. AMIRYAN has previously been convicted of a violation of 8 U.S.C. Section 1326, and has been removed for the U.S. twice. He was last encountered by ICE on February 28, 2017, in Los Angeles County, after having been arrested for possession of credit cards in other persons' names.

IV. PREVIOUS GPS AND BANK ACCOUNT SEIZURE WARRANTS

9. Based on an earlier version of this affidavit, on September 2, 2020, the Honorable Steve Kim, United States Magistrate Judge, issued a GPS/Stingray affidavit for a cellular telephone number used by ANDRANIK AMIRYAN (**Subject Telephone #1**), along with a seizure warrant for bank accounts used to launder fraudulently obtained SBA funds, two of which were in ANDRANIK AMIRYAN's name.

V. STATEMENT OF PROBABLE CAUSE

10. Based on my review of investigative reports and notes, bank statements, witness statements, my discussions with other law enforcement officers working on this investigation, and other evidence, I learned the following information:

A. The Paycheck Protection Program

11. The Coronavirus Aid, Relief, and Economic Security ("CARES") Act is a federal law enacted around March 2020 and was designed to provide emergency financial assistance to the millions of Americans who are suffering the economic effects caused by the COVID-19 pandemic. One source of relief provided by the CARES Act was the authorization of up to $349 billion in forgivable loans to small businesses for job retention and certain other expenses, through a program referred to as the Paycheck Protection Program ("PPP"). Around April 2020, Congress authorized over $300 billion in additional PPP funding.

12. In order to obtain a PPP loan, a qualifying business must submit a PPP loan application, which is signed by an authorized representative of the business. The PPP loan application requires the business (through its authorized representative) to acknowledge the program rules and make certain affirmative certifications in order to

be eligible to obtain the PPP loan. One such certification requires the applicant (through its authorized representative) to affirm that "[t]he [PPP loan] funds will be used to retain workers and maintain payroll or make mortgage payments, lease payments, and utility payments; I understand that if the funds are used for unauthorized purposes, the federal government may pursue criminal fraud charges." In the PPP loan application, the small business (through its authorized representative) must state, among other things, its: (a) average monthly payroll expenses; and (b) number of employees. These figures are used to calculate the amount of money the small business is eligible to receive under the PPP. In addition, businesses applying for a PPP loan must provide documentation showing their payroll expenses.

13. A business PPP loan application is received and processed, in the first instance, by a participating financial institution, then transmitted, for further review, to the Small Business Administration ("SBA") to assess the applicant's eligibility. If a PPP loan application is approved, the participating financial institution funds the PPP loan using its own monies.

14. PPP loan proceeds must be used by the business on certain permissible expenses -- payroll costs, interest on mortgages, rent, and utilities. The PPP allows the interest and principal on the PPP loan to be entirely forgiven if the business spends the loan proceeds on these expense items within a designated period of time (usually eight weeks of receiving the proceeds) and uses at least 75% of the PPP loan proceeds on payroll expenses.

B. ACBA fraudulently received a PPP Loan through FHB using a stolen identity

15. From reviewing loan documents provided by FHB and the SBA, I learned that in or around June 2020, the following loan application was submitted in the name of ACBA for a PPP and EIDL loan:

a. First, the PPP loan application for ACBA was signed by "Petro Kolot" claiming that ACBA was a software development engineering company which reported an average monthly payroll expense of $594,381.84 and a total of 23 employees. The application listed Petro Kolot as the principal of this company and reported that ACBA had been in operation since 2016. The loan application also listed the address for ACBA as 18350 Roscoe Blvd., Northridge, California. As described later, this address is associated with the Northridge Hospital Medical Center and has no relation with ACBA. This loan application was submitted with three tax forms as proof of its employment, IRS Form 941 - Employer's Quarterly Federal Tax. The most recent one was dated on January 31, 2020, and purported to show wages and taxes for ACBA for the last quarter of tax year 2019 in the amount of $594,381. These IRS forms were sent to FHB along with a picture of California Driver License ("CDL") F8214457 purportedly belonging to Petro Kolot.

b. Based on my training and experience, I know that fraudsters will submit doctored IRS forms or documentation that was never actually filed with the IRS to the financial institutions issuing the PPP loans. Fraudsters do so as they are aware that loan officers processing such loans are unable to confirm the information provided with the IRS during the underwriting of the loans.

The CDL Provided to FHB for the ACBA PPP loan is Counterfeit

16. On or about August 26, 2020 I conducted a search on the California Department of Motor Vehicles database for CDL F8214457 and determined that this CDL does not exist.

17. On or about August 26, 2020 I conducted a search on law enforcement databases for personal identifying information matching the ones provided to FHB in the ACBA PPP loan application for Petro Kolot and learned that Petro Kolot has never owned a CDL.

Petro Kolot is a Ukrainian National Who Has Not Travelled to the United States Since 2011

18. On or about August 27, 2020 I conducted a search of US Immigration and Customs databases for Petro Kolot and learned the following:

a. Petro Kolot is a Ukrainian national who was admitted into the United States on or about June 04, 2011 as an Exchange Visitor with a J-1 non-immigrant visa.

b. Petro Kolot remained in the United States for approximately three months and left the United States on or about September 21, 2011.

c. Petro Kolot has not returned to the United States since 2011 nor has he applied for any other visa to travel back to the United States.

19. On or about August 27, 2020 I compared the picture from Petro Kolot Ukrainian passport with the picture found on Petro Kolot counterfeit CDL that was submitted to FHB and determined that they do not look like the same individual.

ACBA Appears to Be a Shell Business

20. On or about August 27, 2020 I conducted a search of ACBA on open source search engines such as google as well as business

networking apps such as Yelp and did not observe any information related to any software development engineering company matching the identifiers provided to FHB.

21. Continuing on August 27, 2020 I reviewed the articles of incorporation for ACBA with the California Secretary of State and learned the following:

a. ACBA was registered on June 16, 2020, and 18350 Roscoe Blvd, Northridge, California is listed as the address of record of the company.

b. ACBA is described as a software programming business.

c. Petro Kolot is listed as Manager and CEO of ACBA.

C. FHB Funded the ACBA loan into a BofA Account Based on the False Information Provided

22. According to bank records, on or about June 30, 2020, FHB funded the ACBA PPP loan, wiring the approved funds to BofA business checking account 325137091308 held in the name of ACBA with Petro Kolot as the sole person with signature authority over the account ("AMIRYAN'S ACBA ACCOUNT 1"), for a total of approximately $ 490,700. (AMIRYAN'S ACBA ACCOUNT 1 was seized pursuant to the previously mentioned warrant.) On or about August 27, 2020, I reviewed the account statements and signature card for AMIRYAN'S ACBA ACCOUNT 1 Account and learned the following:

a. On or about June 19, 2020, ACBA received an initial grant of $10,000 in response to an EIDL request submitted directly with the SBA. This initial disbursement is an advance of funds meant to assist businesses in need as their loan application is getting processed.

b. On or about June 29, 2020, the aforementioned grant

was followed by an additional disbursement of $149,900 which constitutes the full EIDL loan amount paid by the SBA.

c. AMIRYAN'S ACBA ACCOUNT 1 was opened in the name of Petro Kolot on or about June 12, 2020 at a BofA branch located at 7255 Woodman Ave, Van Nuys, California.

D. ATM Photos Show AMIRYAN Depositing Cash into AMIRYAN'S ACBA ACCOUNT 1 on the Day the Account was Opened

23. On or about August 27, 2020, I reviewed ATM footage of an individual later identified as AMIRYAN conducting a $100 ATM cash deposit into the AMIRYAN'S ACBA ACCOUNT 1, on the same day and at the same location that the account was opened.

24. Continuing on or about August 27, 2020, I reviewed California Department of Motor Vehicle records for AMIRYAN. The photo showed the same person I saw on the ATM photos provided by Bank of America during the date listed above.

E. AMIRYAN Transferred $452,287 of Fraud Proceeds from AMIRYAN'S ACBA ACCOUNT 1 to Several Other Businesses and Individual Accounts

25. From reviewing Bank of America documents for AMIRYAN'S ACBA ACCOUNT 1, I learned that a few days after the PPP and EIDL loan funds were deposited into that account, AMIRYAN rapidly transferred the funds by issuing 20 checks drawn against AMIRYAN'S ACBA ACCOUNT 1. The checks were made payable to numerous businesses or individuals. At least two of these accounts are business checking accounts opened with BofA where AMIRYAN is the sole account holder. These accounts, which were seized pursuant to the earlier seizure warrant, received the following checks from AMIRYAN'S ACBA ACCOUNT 1:

a. A check dated July 01, 2020 for $23,980.10 made payable to Magic Finishing at AMIRYAN'S MAGIC FINISHING ACCOUNT 2;

b. A check dated July 09, 2020 for $18,122 made payable to Hetchy Junction at AMIRYAN'S HETCHY JUNCTION ACCOUNT 3.

26. In my training and experience, this pattern is indicative of money laundering; criminals who are trying to move ill-gotten funds will transfer multiple small amounts into other accounts they control or accounts of co-conspirators they are working with, trying to make these transfers look like business transactions among companies or clients.

27. Based on my training and experience, I also know that all of the financial institutions mentioned in this affidavit are federally insured.

F. Magic Finishing and Hetchy Junction are associated with AMIRYAN

28. On or about August 27, 2020, I reviewed the signature cards for the BofA business checking accounts opened in the names of Magic Finishing, LLC. ("AMIRYAN'S MAGIC FINISHING ACCOUNT 2") and Hetchy Junction, Inc. ("AMIRYAN'S HETCHY JUNCTION ACCOUNT 3") and learned the following:

a. AMIRYAN'S MAGIC FINISHING ACCOUNT 2 was opened on November 9, 2018 and lists AMIRYAN as president of Magic Finishing, LLC, and the sole account holder.

b. AMIRYAN'S HETCHY JUNCTION ACCOUNT 3 was also opened on November 9, 2018 and lists AMIRYAN as president of Hetchy Junction, Inc., and the sole account holder.

G. Hetchy Junction Received Fraudulent Funds from a Business called "European Cabinets Direct Import" that Received PPP Funds

29. On or about September 16, 2020 I learned from BofA that on June 22, 2020 a check in the amount of $52,000 drawn against a

business account opened in the name of European Cabinets Direct Import, was deposited into AMIRYAN'S HETCHY JUNCTION ACCOUNT 3. According to BofA, European Cabinets Direct Import received a PPP loan in the amount of 879,852 and depleted all its funds by remitting at least 17 checks for the entire amount of the PPP.

H. Ruse Call to AMIRYAN

30. On or about September 9, 2020 I conducted an undercover phone call to AMIRYAN's telephone (**Subject Telephone #1,** which is tracked pursuant to the earlier warrant), purportedly seeking more information on behalf of the SBA and BofA to release the freeze of AMIRYAN's account and learned the following:

31. The individual who answered the phone identified himself as AMYRIAN and explained that he manufactures cabinets and that the checks remitted from ACBA were payments for products he had sold to a customer by the name of Petro Kolot. AMIRYAN stated that he had met with Petro Kolot and was consequently paid by him in the form of two checks which he then deposited into AMIRYAN'S MAGIC FINISHING ACCOUNT 2 and AMIRYAN'S HETCHY JUNCTION ACCOUNT 3. (Petro Kolot actually left the U.S. in 2011 and has not returned since, as described above.)

32. AMIRYAN stated he was not associated with ACBA and lied about ever conducting any transactions into AMIRYAN'S ACBA ACCOUNT (as described above, there is ATM video of him making the initial deposit on this account on the day it was opened).

I. Hetchy Junction, Magic Finishing, and European Cabinets Direct Imports appear to be Sham companies

33. On or about September 17, 2020 I learned from BofA that Hetchy Junction, Magic Finishing, and European Cabinets Direct

Imports are entities that purport to specialize in cabinet making, however, the account activity for these accounts does not show any expenses consistent with cabinet making or woodcraft businesses. For example, I did not observe the purchase of raw materials commonly used in cabinet making.

J. AMIRYAN Called BofA Using Subject Telephone #1 to Inquire About the Status of His Bank Accounts.

34. According to bank records, on or about August 27, 2020 AMIRYAN contacted BofA from phone number 310-944-4401 **Subject Telephone 1** to inquire about the status of AMIRYAN'S MAGIC FINISHING ACCOUNT 2 and AMIRYAN'S HETCHY JUNCTION ACCOUNT 3, which were frozen by BofA a few days earlier. AMIRYAN was told that he would be contacted by a BofA bank investigator at a later date to discuss the reason behind the accounts freeze.

35. On or about August 27, 2020 I learned from BofA that **Subject telephone 1** is listed in the BofA user profile of AMIRYAN for both AMIRYAN'S MAGIC FINISHING ACCOUNT 2 and AMIRYAN'S HETCHY JUNCTION ACCOUNT 3 as his personal cellphone number.

K. ACBA's Address Is an Address Associated with the Northridge Hospital Medical Center

36. On or about August 20, 2020 HSI SA Masood Azaran conducted surveillance at 18350 Roscoe Boulevard, Northridge, California – an address that was reported as ACBA company's address in the PPP loan application provided to FHB - and learned the following:

a. The building is associated with the Northridge Hospital Medical Center and it is managed by Healthcare Management of America, Inc.

b. The building's directory does not list any company by the name of ACBA.

c. None of the companies listed in the building's directory operate in any field other than healthcare.

L. AMIRYAN Has a Criminal History and History With Fraud

37. During the course of my investigation I reviewed the criminal history for AMIRYAN and learned the following:

a. AMIRYAN has a criminal history dating back to in or about 2002 which includes convictions related to burglary, false personation of another, and grand theft, as recently as 2017.

b. In 2008, AMIRYAN was removed to Armenia by Immigration Customs Enforcement – Enforcement Removal Operations ("ERO") for being an aggravated felon and, upon illegal re-entry, was removed again in 2011. In 2017 AMIRYAN was reinstated after illegally reentering once again through the South-Western border at an unknown time. AMIRYAN appears to have a pending Stay of Removal and is currently enrolled with ERO in "alternative to detention," meaning that he has been released on bond but must comply with special rules and restrictions, similar to someone who has been released on bond from criminal charges.

M. AMIRYAN resides at AMIRYAN'S RESIDENCE

38. On or about September 11, 2020, I received information from ERO that as part of AMIRYAN's supervised released with Immigration Customs Enforcement ("ICE"), AMIRYAN has reported his address to be located at AMIRYAN'S RESIDENCE.

39. Continuing on September 11, 2020, I reviewed the application of AMIRYAN's Application for Employment Authorization with the United States Citizenship and Immigration Services ("USCIS") dated April 4, 2019 and learned that AMIRYAN's address is listed as AMIRYAN'S RESIDENCE.

40. On September 15, 2020, I reviewed the GPS pings for **Subject Telephone #1** which have been provided by Verizon Wireless at intervals of fifteen minutes since on or about September 10, 2020 and learned the following:

a. the GPS pings for **Subject Telephone #1** often correspond to geographical coordinates located within a few meters of AMIRYAN'S RESIDENCE, which is within the radius of uncertainty for the pings. That is, while the pings are not located at AMIRYAN'S RESIDENCE, they are consistent with the expected coordinates if **Subject Telephone #1** were located at AMIRYAN'S RESIDENCE.

N. Counter Surveillance at AMIRYAN'S RESIDENCE

41. On September 16, 2020, I conducted surveillance in the vicinity of the GPS pings and observed the following:

a. AMIRYAN'S RESIDENCE is a single-family house surrounded by a boarded fence and a secured pedestrian gate which greatly reduce visibility of the inside of the property. AMIRYAN'S RESIDENCE appears to be monitored by at least three cameras overlooking the lawn and OSWEGO STREET and an additional Ring camera affixed by the pedestrian gate. AMIRYAN'S RESIDENCE is also equipped with a motion detecting light which activates anytime someone walks in front the pedestrian gate. Additionally, AMIRYAN'S RESIDENCE has "beware of dog" signs; as I approached the fence, I heard barking and saw the shadows of what appeared to be two large dogs that ran up to the fence where I was.

b. Based on my training and experience, security features such as the ones described above mean that the occupants of the house are concerned with the presence of evidence of illegal activity and/or the presence of contraband stored inside their property.

c. I saw a purple Dodge Challenger leave the driveway of AMIRYAN'S RESIDENCE bearing CA license plate 8PRN152. The vehicle drove away AMIRYAN'S RESIDENCE and left the area. Within minutes, the Challenger returned to the area and stopped in the middle of the street next to my vehicle, which is an undercover police vehicle and looks like it. No vehicle was in front of the Challenger impeding its travel. After a few seconds, the Challenger drove toward the SUBJECT RESIDENCE, made a U turn, without entering the driveway at the SUBJECT RESIDENCE and drove directly to the front of my vehicle and stopped in the middle of the street. Again, no traffic was impeding the Challenger from driving. The Challenger had tinted windows, but the car was close enough that I could see that the driver was a female. After a few seconds, the Challenger drove away out of the area. On or about September 16, 2020, I reviewed the California Law Enforcement Telecommunication System database and found that the vehicle bearing California license plate 8PRN152 was a Dodge 2020 leased to "Hetchy Junction Inc", the name of one of the purported businesses that AMIRYAN used in his PPP fraud and money laundering scheme. Based on my training and experience, I believe the driver of the Challenger worried that my undercover vehicle indicated that law enforcement was interested in AMIRYAN'S RESIDENCE, and returned to check out me and my vehicle. (I pretended to be occupied with something inside my car when the Challenger checked me out, and then drove away after it left.)

d. A few minutes after the Challenger checked me out, SA Orrantia saw AMIRYAN (identified by his driver's license photograph and bank surveillance photographs) exit the pedestrian gate of

AMIRYAN'S RESIDENCE and look west toward where my government vehicle had been parked.

O. AMIRYAN'S RESIDENCE Is Associated with Other Frauds

42. I reviewed the results of a search on Westlaw's public records database regarding 8442 OSWEGO, SUNLAND (AMIRYAN'S RESIDENCE) and found an impossibly high number of death records. For example, it reported seven separate deaths on September 4, 2020, alone. For September 3, 2020, the number of reported deaths was 49. That other time I encountered a residence with an impossibly high number of reported deaths associated with it, it turned out to used by Arman Manukyan, who was engaged in bulk unemployment benefits fraud. I recovered multiple EDD cards in other persons' names from his residence in Van Nuys during the execution of a federal search warrant there, and separately observed him going from ATM to ATM withdrawing cash using still other EDD unemployment benefits cards previously. According to travel records, Arman Manukyan flew from Mexico to Belarus, a country with which the U.S. has no extradition treaty, shortly thereafter. There is no record of Manukyan crossing the U.S. border into Mexico, but he must have done so. Manukyan remains a fugitive from a federal complaint.

43. On or about September 18, 2020 I learned from JPmorgan Chase Bank that an individual by the name of Meline Ghazarian (who according to property records is the owner of AMIRYAN'S RESIDENCE), was witnessed on or about August 30, 2016, withdrawing approximately $40,000 in cash in increments of $9,900 at a branch located in Glendale after being advised by the teller of the Currency Transaction Report ("CTR") requirements established by the Bank Secrecy Act. According to this regulation, financial Institutions

are required to electronically file a CTR for each transaction in currency (deposit, withdrawal, exchange, or other payment or transfer) of more than $10,000. Based on my training experience, individuals engaged in illicit activities often attempt to circumvent financial reporting requirements to hide from law enforcement and Anti money laundering bank investigators. According to Meline Ghazarian's criminal history report, she was convicted of Grand Theft Property in 2007.

44. On or about September 18, 2020 I learned from Wells Fargo that two individuals received two EIDL loans in the amount of $139,900 and $144,900 respectively. As with AMIRYAN's fraudulent loans, these sums were rapidly withdrawn through eight outgoing checks totaling $164,500, in amounts ranging from $5,000 to $42,000, which were deposited into a business checking account opened in the name of AAA Painting & Flooring Inc. According to Westlaw records, this purported business is located at AMIRYAN'S RESIDENCE. According to bank records, Artak AMIRYAN (likely a relative of ANDRANIK AMIRYAN) has sole signature authority over the AAA Painting & Flooring Inc., and his address is AMIRYAN'S RESIDENCE. I reviewed California Department of Motor Vehicle records for Artak AMIRYAN and learned that AMIRYAN'S RESIDENCE is listed on his driver's license as his residence since on or about January 17, 2020.

P. AMIRYAN Illegally Re-Entered the U.S. After Removal

45. I reviewed ICE records which show that AMIRYAN (identified by both his name and date of birth) obtained a visa to enter the U.S. in 1997. Photographs of his Armenian passport and U.S. visa both indicate that his nationality is Armenian. According to both his criminal history report, and ICE records, AMIRYAN sustained felony

convictions in two separate cases, both of which were completed on January 30, 2007, and presumably consolidated for sentencing:

a. In the first case, which stemmed from an arrest on April 1, 2004, AMIRYAN was ultimately convicted of Burglary, in violation of California Penal Code Section 459, and Get Credit/Goods in Another's Identity, in violation California Penal Code Section 530.5, for which he was sentenced to two years in prison.

b. In the second case, which stemmed from an arrest on February 14, 2006, AMIRYAN was ultimately convicted of Grand Theft, in violation of California Penal Code Section 487, and False Personation of Another, in violation of California Penal Code Section 529, for which he was sentenced to three years in prison.

c. (According to his criminal history, the arrests in both of those case occurred while AMIRYAN was on probation for theft, which began on April 23, 2003, and lasted 36 months.)

46. ICE records show that AMIRYAN was deported to Armenia on April 16, 2008, after he was released from prison on the offenses mentioned above.

47. On or about November 26, 2009, AMIRYAN was charged as Illegal Alien Found After Removal and Conviction, in violation of 8 U.S.C. § 1326, for which defendant was later sentenced to 14 months in prison, and three years of supervised release beginning in December of 2010. ICE records further show that AMIRYAN attempted to illegally re-enter the U.S. from Canada in 2011, when he was on supervised release for his Section 1326 conviction.

48. There is no indication in AMIRYAN's ICE records that he ever applied for, or received from the Attorney General or the

Secretary of Homeland Security, permission to legally re-enter the United States following his removals.

49. According to a Glendale police report, AMIRYAN was arrested in that city on February 28, 2017, for possessing credit cards in other persons' names. Per ICE records, immigration learned of his presence in the country that same day.

50. Continuing on or about February 28, 2017, during the course of the interview with ERO Deportation Officer Rachel, AMIRYAN admitted that he entered the United States by sneaking across the Mexican border at an unknown time.

51. According to ICE records, on February 12, 2018, AMIRYAN had "PASSPORT NO. Am0446567, [which] Expires 09/06/2021." The writer emphasized: "Please note Name on Passport (GHAZARYAN, Andranik) nb." As described previously, AMIRYAN had initially entered the U.S. on a passport in the name ANDRANIK AMIRYAN, so it appears that after he was deported to Armenia, he secured there a new Armenian passport in an alias and brought it back with him to the U.S. when he illegally re-entered.

52. As described earlier, AMIRYAN was released from ICE custody on bond, and is currently challenging his removal order in the Ninth Circuit. From talking to ERO Supervisory Detention Officer Crook I know that one of the conditions of release is that he not commit any new offenses. Supervisory Detention Officer Crook also told me that he had discretion to revoke AMIRYAN's immigration bond and hold him in ICE custody based on the evidence I had gathered of his fraud, and would do so. I asked him to wait until after I had arrested AMIRYAN.

VI. TRAINING AND EXPERIENCE REGARDING THE SUBJECT OFFENSES

53. Based on my experience and training, and based on my consultation with other law enforcement officers, I know that:

a. Individuals involved in fraud schemes like this one usually keep evidence of their schemes, such as pay-owe sheets for dividing the proceeds, contact information for their co-conspirators, and records documenting the scheme so when an error is made, they can recreate the documentation needed to help conceal the fraud.

a. These individuals often use the proceeds of the fraud to purchase expensive items, or store the proceeds in the form of cash to make it more difficult to trace.

b. Based on my training and experience in the field of financial crimes investigations, I also know that it is common for identity thieves to exploit the Federal CARES Act, meant to bring financial relief for individuals and entities affected by COVID-19. Identity thieves know that money is often expediently dispensed and with little oversight. Identity thieves who exploited loans and grants offered by the SBA will also do the same with the California Employment Development Department by obtaining the Personal Identifying Information "PII" of California residents, and fill out online EDD applications for those residents, unbeknownst to, and without the permission of the resident. The identity thief will typically file multiple fraudulent applications and list mailing addresses that allow the identity thieves easy access, while adding another layer of anonymity, such as a nearby house where the resident does not check the mail regularly, or a collusive third party. EDD will mail an EDD Debit Card, administered by Bank of America, to the listed address. Fraudsters may immediately activate their card via an

automated telephone service and begin using it anywhere VISA cards are accepted. Fraudsters can also simply visit multiple Automated Teller Machines "ATMs" to withdraw funds directly. Based on your affiant's training and experience in the field of identity theft investigations, your affiant knows it is common for identity thieves to often employ multiple collusive parties to visit multiple ATMs on their behalf. This adds an additional layer of anonymity to their scheme and helps to avoid detection and identification via video surveillance.

c. Individuals involved in fraud schemes need to communicate with their co-conspirators about their fraudulent activity. There are usually records of those communications in their electronic devices such as cellular telephones.

d. Typically, they maintain the evidence where it is close at hand and safe, such as in their residences, vehicles, and digital devices, which are also commonly stored in their residences and vehicles. Such individuals commonly use digital devices to communicate with their fellow participants by phone, email and text messages. I know that individuals who commit crimes with the aid of electronic devices do not readily discard them, as computers, tablets and cell phones are expensive items that are typically used for years before being upgraded or discarded. Computers, tablets and cell phones can be used to communicate between co-conspirators and may contain information relating to the crime under investigation.

e. I know from training and experience that individuals involved in fraud keep the most damaging evidence and/or proceeds of the scheme at their residences, vehicles, garages and to help conceal the fraud from their fellow coworkers who may have access to such

documents at the workplace. Proceeds such as cash and gifts are easier to conceal at the fraudster's residence rather than in plain view of coworkers. More sophisticated or cagey criminals may rent public storage units to use to further distance themselves from incriminating evidence, or safety deposit boxes, especially when storing valuables such as cash.

VII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

54. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores

files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

55. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take

substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

56. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a

biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress the thumb and/or fingers of ANDRANIK AMIRYAN, Artak Amiryan, and Meline Ghazarian on the device(s); and (2) hold the device(s) in front of those persons' faces with their eyes open to activate the facial-, iris-, and/or retina-recognition feature.

57. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VIII. CONCLUSION

58. Based on the facts described above, there is probable cause to believe that ANDRANIK AMIRYAN violated 8 U.S.C. Section 1326, and 18 U.S.C. Sections 1344, 1349, and 1028A, and that the items listed in Attachment B are evidence, fruits, and instrumentalities of the SUBJECT OFFENSES, and will be found at AMIRYAN'S RESIDENCE.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 23rd day of September, 2020.

UNITED STATES MAGISTRATE JUDGE

Hon. Michael R. Wilner