# UNITED STATES DISTRICT COURT

for the

Central District of California

| | | |
|---|---|---|
| In the Matter of the Search of<br>*(Briefly describe the property to be searched or identify the person by name and address)*<br>BLACK 2024 LAND ROVER RANGE ROVER SPORT P400 BEARING California license plate 9MNG093, VIN SAL1L9FU5RA404809 | ) | Case No. 2:24-MJ-7120 |

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

*See Attachment A*

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

*See Attachment B*

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☒ evidence of a crime;

☒ contraband, fruits of crime, or other items illegally possessed;

☒ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| 18 U.S.C. §§ 1341, 1343, 1344, 1349, 1956, and 1546 | See affidavit |

The application is based on these facts:

*See attached Affidavit*

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (*give exact ending date if more than 30 days*: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s Jenae Combest-Smith

*Applicant's signature*

Special Agent Jenae Combest-Smith , HSI

*Printed name and title*

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

Date: _____

*Judge's signature*

City and state: Los Angeles, CA

Hon. Margo A. Rocconi, U.S. Magistrate Judge

*Printed name and title*

AUSA Andrew Brown, x0102, 11th Floor

**ATTACHMENT A-2**

THE VEHICLE TO BE SEARCHED IS:

The BLACK 2024 LAND ROVER RANGE ROVER SPORT P400 bearing California license plate 9MNG093, and VIN SAL1L9FU5RA404809 (the "SUBJECT VEHICLE").

**ATTACHMENT B**

**I. ITEMS TO BE SEIZED**

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 1341, 1343, 1344, 1349, 1956, and 1546 (conspiracy to commit mail, wire, and bank fraud, money laundering, and passport fraud), collectively referred to as the "SUBJECT OFFENSES," namely:

a. Documents and records referring or relating to establishing or maintaining business websites, such as S&S Auto Sales and Dennis Polk Equipment, advertising vehicles for sale, the offer or sale of vehicles including farming equipment, and photographs of vehicles of the type commonly used to advertise vehicles for sale;

b. Personal identifying information of individuals other than those residing at 4827 RIVERTON AVENUE, NORTH HOLLYWOOD, CALIFORNIA 91601, including social security numbers, other identifying numbers, dates of birth, addresses and telephone numbers, credit, gift, or debit card information, PINs, credit reports, and bank or other financial institution information, and records referring or relating to such information;

c. Counterfeit identity documents, such as passports and driver's licenses, whether blank, completed, or partially completed, and their components, such as seals, watermarks, security windows, official signatures or the cutting-and-pasting of signatures, holographic security features, ultraviolet printed features, raised micro dot features, and translucent Teslin printed design components, identification-proportioned photographs of faces, and programs or records referring or relating to them;

d. Credit and debit cards not in the names of the residents of 4827 RIVERTON AVENUE, NORTH HOLLYWOOD, CA 91601, cards with magnetic strips that are commonly overwritten to produce counterfeit access devices, such as gift cards with no value on them (which will be determined after the search) or blank card stock, any card for which the embossing or information on the front does not match the information recorded on the magnetic strip on the back (which will be determined after the search), any card with a PIN written on it or attached to it, lists of PINs, and records or documents referring or relating to the same;

e. Equipment and objects used to skim, shim, or counterfeit credit or debit cards, such as embossers, encoders, ultraviolet printing devices, tipping foil, magnetic card readers or writers, credit card chip readers and writers, blank cards containing magnetic strips or chips, related equipment or materials such as chips, magnetic strips, images of debit or credit cards, portable media storage devices, holographic stickers, partially completed credit or debit cards, and documents, records, or programs that refer or relate to them;

f. Miniature or spy cameras or surveillance equipment that could be used to capture PINs, equipment to install or mount them, including magnets, or to record or transmit their images, and documents, records, and programs, referring or relating to them including the data they record;

g. Blank or partially completed credit and debit cards, cards with magnetic strips that are commonly overwritten to produce counterfeit access devices, such as gift cards with no value on them (which will be determined after the search) or blank card stock, any

card for which the embossing or information on the front does not match the information recorded on the magnetic strip on the back (which will be determined after the search), any card with a PIN written on it or attached to it, lists of PINs, and records or documents referring or relating to the same;

h. Equipment designed to produce identity documents, cards, or access devices, or their security features, such as card printers, embossers, encoders, magnetic card readers or writers, credit card chip readers and writers, their components and supplies, such as blank card stock, tipping foil, Teslin sheets, holographic printing supplies, ultraviolet printing supplies, and records or programs that refer or relate to them;

i. Documents and records referring or relating to machine shops, metal working, sheet metal, or the custom manufacture of mechanical or electronic devices;

j. Records, programs, and items relating to the counterfeiting or manipulation of documents and identifications, such as the cutting-and-pasting of signatures, forging or copying passports, driver's licenses, and other form of identification, identification-proportioned photographs of faces, letterheads, watermarks, and seals, including the altered or counterfeited information itself.

k. Documents, records, and programs referring or relating to ATMs including their locations and cash withdrawals or advances, and pay/owe sheets;

l. Documents, records, and programs referring or relating to international transfers of funds, international travel or visas including illegal border crossing and the smuggling of persons,

international shipping or packages, foreign financial accounts, and citizenship or alienage;

m. Documents, records, and images showing members of the conspiracy associating or communicating with each other or with the unidentified persons also captured on ATM surveillance photographs;

n. Documents and records referring or relating to the conversion of cash to financial instruments such as checks and wire transfers, and vice versa, for a percentage of the dollar value converted, or the transfer of cash abroad, such as through Hawalas or money transferring businesses, like Western Union, or the purchase of cryptocurrency for cash;

o. Mail matter and shipping packages, opened or unopened, not addressed to or from 4827 RIVERTON AVENUE, NORTH HOLLYWOOD, CA 91601, and documents or records referring or relating to the same;

p. Currency, prepaid debit or credit cards, and casino chips with a value in excess of $1,000, including the first $1,000 if more than $1,000 is found;

q. Documents and keys relating to public storage units, rental cars, prepaid cellular telephones, safety deposit boxes, Commercial Mail Receiving Agencies, or receiving mail or deliveries at someone else's address;

r. Records referring or relating to counter surveillance of law enforcement, jail or prison, arrests, criminal investigations, criminal charges, asset forfeiture, investigations by financial institutions, and the threatened or actual closure of accounts by financial institutions;

s. Documents and records referring or relating to currency transaction reports (CTRs), their reporting thresholds,

attempting to structure cash transactions to avoid CTRs, cash transactions totaling over $10,000 even if conducted in lesser increments, or the purchase of more than $3,000 of postal money orders in a two-week period, or conducting multiple cash ATM transactions or purchasing multiple postal money orders on the same day;

t. Documents and records referring or relating to the conversion of cash to financial instruments such as checks and wire transfers, and vice versa, for a percentage of the dollar value converted, or the transfer of cash abroad, such as through Hawalas or money transferring businesses, like Western Union, or the purchase of cryptocurrency for cash;

u. Records relating to wealth and the movement of wealth since 2022, such as tax returns and forms, crypto-currency accounts and transfers, other digital wealth storage and transfer methods including PayPal and Venmo, money orders, brokerage and financial institution statements, wire transfers, currency exchanges, deposit slips, cashier's checks, transactions involving prepaid cards, and/or other financial documents related to depository bank accounts, lines of credit, credit card accounts, real estate mortgage initial purchase loans or loan refinances, residential property leases, escrow accounts, the purchase, sale, or leasing of automobiles or real estate, or auto loans, and investments, or showing or referring to purchases or transactions for more than $1,000;

v. Records or items containing indicia of occupancy, residency or ownership of any location or vehicle being searched, such as keys, rental agreements, leases, utility bills, identity documents, cancelled mail, and surveillance video;

w. Documents and records showing electronic and telephone contacts and numbers called or calling, such as SIM cards, address books, call histories, telephone bills, and Signal, ICQ, Telegram, and email addresses.

x. Cryptocurrency and related records and items, such as those referring or relating to public or private keys or addresses, or cryptocurrency wallets or their parts, including "recovery seeds" or "root keys" which may be used to regenerate a wallet. Seizure of the cryptocurrency and wallets will be accomplished by transferring or copying them to a public cryptocurrency address controlled by the United States, or by restoring them onto computers controlled by the United States.

y. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the SUBJECT OFFENSES, and forensic copies thereof.

2. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

a. evidence of who used, owned, or controlled the device 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, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

b. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of

the presence or absence of security software designed to detect malicious software;

c. evidence of the attachment of other devices;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

e. evidence of the times the device was used;

f. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

g. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

h. records of or information about Internet Protocol addresses used by the device;

i. records of or information about the device'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.

3. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

4. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless

communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

**II. SEARCH PROCEDURE FOR DIGITAL DEVICES**

5. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the

items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team will not search for similar evidence outside the scope of the items to be seized without first obtaining authority to do so.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1)itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may

retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

6. The review of the electronic data obtained pursuant to this warrant 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 investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

7. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device

a. During the execution of this search warrant, law enforcement is permitted to: (1) depress the thumbs and/or fingers of MIHAI TRIF, and any other adult located at the SUBJECT PREMISES during the execution of the search who is reasonably believed by law enforcement to be a user of a biometric sensor-enabled device that falls within the scope of the warrant, 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 the faces of those persons 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.

8. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant, and do not apply to any other search of digital devices.

**AFFIDAVIT**

I, Jenae Combest-Smith being duly sworn, declare and state as follows:

**INTRODUCTION**

1. I am a Special Agent with Homeland Security Investigations ("HSI") in Los Angeles, California, and have been so employed since May 2022. To become an HSI Special Agent, I completed six months of training at the Federal Law Enforcement Training Center in Brunswick, Georgia.

2. During my employment as an HSI Special Agent, I have participated in investigations related to narcotics smuggling, organized criminal activity, document fraud, sex trafficking, human smuggling, and other financial related crimes. I have participated in various aspects of criminal investigations, including telephone records analysis, physical surveillance, search warrants, seizures of narcotics, electronics, documents, skimming devices, and reviewing evidence from those seizures. I have also spoken to and interacted with many law enforcement agents who have prior knowledge and experience investigating financial related crimes and the methods used to commit those crimes.

3. Prior to becoming a Special Agent with HSI, I was employed as an insurance fraud investigator for approximately 12 years in the private sector. During my employment as an insurance fraud investigator, I investigated fraudulent insurance claims and was responsible for reporting fraudulent claims to designated government and law enforcement agencies for further investigation and prosecution

4. I also have extensive experience investigating Romanian Transnational Criminal Organizations (TCO). I have conducted investigations in the Los Angeles area related to various fraud crimes and money laundering, and I have also traveled to Romania to share information and coordinate investigations with HSI Bucharest and Romanian law enforcement regarding Romanians who travel from Romania and Europe to the United States to defraud victims.

## I. PURPOSE OF AFFIDAVIT: SEARCH WARRANTS

5. This affidavit is made in support of search warrants for the residence and vehicle of MIHAI TRIF for evidence of conspiracy to commit mail, wire, and bank fraud, money laundering, and passport fraud, in violation of Title 18 U.S.C. §§ 1341, 1343, 1344, 1349, 1956, and 1546 (collectively, the "SUBJECT OFFENSES"), as described in Attachment B.

6. The information set forth in this affidavit is based upon my participation in the investigation, encompassing my personal knowledge, observations and experience, as well as information obtained through my review of evidence, investigative reports, and information provided by others, including other law enforcement partners. As this affidavit is being submitted for the limited purpose of securing the requested warrants, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause for the requested warrants.

## II. PREMISES AND VEHICLE TO BE SEARCHED

7. The premises and vehicle to be searched are:

a) The residence located at 4827 RIVERTON AVENUE, NORTH HOLLYWOOD, CALIFORNIA 91601 (the "**SUBJECT RESIDENCE**"), described more fully in Attachment A-1, which is incorporated by reference.

b) The BLACK 2024 LAND ROVER RANGE ROVER SPORT P400 BEARING California license plate 9MNG093, VIN SAL1L9FU5RA404809, registered to EAN Holdings, and driven by MIHAI TRIF ("**SUBJECT VEHICLE**"), described more fully in Attachment A-2, which is incorporated by reference.

## III. ADDITIONAL INFORMATION ABOUT FINANCIAL FRAUD

8. I have conducted financial investigations involving sophisticated money laundering techniques and fraud. Through training and experience, I have become familiar with how those engaged in fraudulent activity obtain identifying information of victims, such as a full name, date of birth and social security number, and then use that information to open numerous bank and credit card accounts. I know that individuals that commit fraud maintain victim information and other information relevant to the fraud scheme for long periods of time because it is of value in perpetuating additional acts or further fraud schemes. The purpose of opening accounts (i.e., bank, email, phone, etc.) is to further a fraud scheme, which often involves several co-conspirators. The goal of this scheme is to defraud banks, merchants, and victims to obtain cash or other items of monetary value such as gift cards and electronics. These items are often sought out due to their high liquidity. During account openings, those individuals committing fraud typically provide fictitious and/or fraudulent identities and a mailing address that

they exercise control over to obtain a bank issued debit or credit card in furtherance of the fraud scheme, often using post mailboxes or third-party mail receipt services to elude detection by law enforcement. Due to the complexity of the fraud, the sheer number of victims, and criminal conduct spanning multiple jurisdictions, it is not uncommon for these financial fraud crimes go unsolved and/or uninvestigated. This scheme requires the perpetrators to be in communication, which is often done via cell phone(s) and/or VoIP phones. Additionally, those involved in fraudulent acts and schemes generally use a computer to facilitate the scheme by setting up email accounts, setting up VoIP accounts, applying for bank accounts and credit cards online, or other necessary things to make the scheme successful, such as manufacturing counterfeit identification documents, altered and/or counterfeit checks, credit cards, or other financial instruments.

## IV. ADDITIONAL INFORMATION ABOUT ROMANIAN TRANSNATIONAL CRIMINAL ORGANIZATIONS (TCO)

9. Members of Romanian TCOs are trained to travel from Romania and Europe to the United States to defraud Americans, United States government programs, and the United States banking system. Members of Romanian TCOs often stay in the United States illegally for many years while they commit these crimes. Oftentimes, members travel back and forth from the United States but re-enter and exit illegally in order to evade law enforcement. Members are trained to import fraudulent identification documents to assist them with their crimes and launder money for the TCO with the goal to re-integrate it into the Romanian banking system and real estate. This has been

corroborated by intelligence received from Romanian law enforcement along with my training and experience on Romanian TCOs.

10. Members of Romanian TCO fraud groups typically enter the country either legally with a visa, if they have no criminal record and can pose as a legitimate tourist or businessperson, or through established immigrant-smuggling rings in Mexico and Canada otherwise. Oftentimes the crew members maintain false identity documents, which they use if arrested to make it harder to identify them. Some maintain false passports so that they can abscond if granted bail and flee the country.

11. Members of Romanian TCO fraud groups have various ways of handling the proceeds of their offenses. Some is kept in cash for routine expenses. Some is usually deposited into a local bank account to pay for items for which cash would raise suspicion, such as rental cars and housing. The bulk, however, is sent abroad either to their co-conspirators or home countries. This may be as simple as sending cash hidden among other items abroad through carriers such as DHL, or transfers through banks, Hawalas, Western Union, or similar services. More recently, the trend has been to purchase cryptocurrencies for cash.

12. Members of Romanian TCOs involved in fraud schemes must keep evidence of their schemes, such as contact information for their co-conspirators, lists of victim information and accounts used in the scheme, simply to keep the scheme going. Much of this evidence is now stored on digital devices such as computers and smartphones.

13. Generally, perpetrators of fraud and identity theft schemes maintain this evidence where is close at hand and safe, such as in

their residences, automobiles, and, especially with smartphones, on their person. For larger or more sophisticated frauds, participants often attempt to distance themselves from some of the incriminating evidence by renting public storage units or safety deposit boxes where they often keep the items they will not need immediate access to.

14. Members of Romanian TCOs must out of necessity communicate with one another. Commonly this is done by text, VOIP, email, telephone, or specialty communication application, often an encrypted one such as WhatsApp, and most often by smartphone. Members of the conspiracy commonly carry their smartphones, which include the contact information for their co-conspirators, on or near their persons, such as in their cars or residences.

## V. STATEMENT OF PROBABLE CAUSE

15. Homeland Security Investigations (HSI) Los Angeles, HSI Pensacola, HSI Attaché Bucharest, HSI Attaché Vienna, United States Secret Service (USSS) San Diego, and Romanian Law Enforcement (hereinafter collectively referred to as "Investigators") are currently investigating a Romanian Transnational Criminal Organization (TCO). I am the assigned case agent and have been directly involved with the investigation for approximately 18 months.

16. In summary, the investigation has revealed that members of this Romanian TCO operate various organized crimes groups that have specializations including human smuggling, narcotics smuggling, money laundering, import and export violations, organized retail theft, gambling, prostitution, violence, credit-card skimming, and financial fraud schemes domestically and internationally. Investigators have

identified numerous members of this Romanian TCO, including a Romanian national identified as MIHAI TRIF, DOB: XX/XX/1993.

17. The investigation to date has revealed that TRIF likely unlawfully entered the United States within the last 24 months, most likely from Canada. Specifically, I have received information from Canadian authorities showing that TRIF entered Canada via Montreal International Airport on September 9, 2022, from Paris, France. TRIF was granted entry into Canada as a visitor and used a valid Romanian passport.

18. I have conducted queries in law enforcement databases and have been unable to locate any lawful entry and subsequent admission into the United States after TRIF's entry into Canada on September 9, 2022. Based on my training and experience, I know that it is common practice for members of Romanian TCOs and other illegal aliens engaged in criminal activity to enter the United States illegally through Canada or Mexico in order to evade law enforcement Thus, TRIF is illegally present in the United States with no lawful status.

19. In the United States, TRIF has at least two arrests with no dispositions in California, including a February 2023 misdemeanor arrest for Petty Theft and a June 2023 felony arrest for Inflict Corporal Injury to Spouse / Cohabitant, referencing FBI No XXXXXXPAL and California State ID XXXXX888. The prosecution status of both cases is currently unknown to me. As detailed herein, these arrests were made after TRIF unlawfully entered the United States at some time after September 9, 2022. Despite TRIF's immigration status, the arresting agencies had no legal authority to question TRIF's immigration status. Additionally, TRIF was arrested in the state of

California, which is regarded as a "sanctuary state".[1] Thus, immigration authorities were not aware of TRIF's arrest and subsequent temporary detention.

20. As detailed herein, Investigators and my subsequent investigation have identified at least 15 fraudulent and fictitious identities directly attributable to TRIF and TRIF's fraud schemes. Several of the identities were identified prior to TRIF using them (i.e., actively targeting inbound international shipments that seized the fraudulent documents), several of the identities were identified after-the-fact as part of a historical financial investigation, and at least two are currently being proactively investigated as newly assumed identities that TRIF is believed to be actively using, including one as part of a new Confidence Fraud Scheme (i.e., "Karel TOKAR") and another as an identity TRIF is using to lauder illicit proceeds and elude detection by law enforcement (i.e., "Ivan BUGATZI").

21. For purposes of this affidavit, I have conducted an in-depth analysis of TRIF's three most recent identities, including "Marek BALVIN", "Karel TOKAR", and "Ivan BUGATZI". These three identities are recent and relevant to my ongoing investigation into TRIF and TRIF's fraud schemes several ways and encompasses the relevant period of August - Present.

22. At this time, TRIF's full role in the fraud schemes is currently unknown; however, the investigation revealed that TRIF at a minimum is responsible for creating fictitious and fraudulent

[1] In April 2017, the California State Senate approved a bill that increased protections for immigrants. The measure prohibits local law enforcement agencies from using resources to investigate, detain, report or arrest people for immigration violations.

identities and opening and maintaining financial accounts used to directly receive wire transfers from victims. TRIF then immediately withdraws and spends the funds from swindled victims. While it appears that TRIF is organizing the scheme, based on my training, experience, and investigation to date, I believe that TRIF's fraud schemes are complex and likely involves multiple unknown co-conspirators. For example, some victims reported talking to both a male and female scammer by telephone.

23. First, "Marek BALVIN" was identified as an identity used to swindle at least six victims out of $141,278 in September 2024 using two U.S. financial institutions, including Wells Fargo Account XXXXXX5272 ("WF 'BALVIN' Account-5272") and Citibank Account XXXXX7684 ("Citibank 'BALVIN' Account-7684"). Both accounts were opened in August 2024 in the greater Los Angeles, CA area using the fictious identity and supporting fraudulent documents of "Marek BALVIN". I have provided still frame CCTV images from the Citibank 'BALVIN' Account-7684 showing that an individual I have identified by sight as TRIF was captured opening the account on August 22, 2024, and subsequently withdrawing funds via teller and ATM from the account on September 9, 11, 13, and 17, 2024. The fund source was from two separate victims that wired $15,000 and $16,000 on or about September 9, 2024. The two victims were confirmed through victim interviews and identified in North Dakota and New Jersey, respectively. The victim funds were immediately withdrawn by TRIF from a branch and ATM located less than 4 miles from the **SUBJECT RESIDENCE**.

24. Second, "Karel TOKAR" was identified as a new replacement identity used by TRIF as part of a new and ongoing fraud scheme. I identified "Karel TOKAR" by conducting an analysis of the identity "Marek BALVIN," including a phone analysis and other investigative techniques. The subsequent analysis identified the identity of "Karel TOKAR" and the suspected cellular phone attributable to the identity, identified as (818) 605-2154 ("TRIF's 'TOKAR' Phone-2154"). I positively identified TRIF as the user and holder of TRIF's 'TOKAR' Phone-2154 via subsequent court authorization geolocation of TRIF's 'TOKAR' Phone-2154 in conjunction with physical surveillance in November 2024 and other investigative techniques. This also assisted in identifying the **SUBJECT RESIDENCE** and the **SUBJECT VEHICLE**. The identification of "Karel TOKAR" was exclusively established by the initial identification of "Marek BALVIN". This is strong evidence to indicate that the identities are intertwined and directly related to each other.

25. Third, "Ivan BUGATZI" was identified as TRIF's alias to launder his illicit proceeds and to live day-to-day in an attempt to elude detection by law enforcement. I identified "Ivan BUGATZI" by court authorization geolocation of TRIF's 'TOKAR' Phone-2154 in conjunction with physical surveillance and a review of CCTV footage in November 2024. These investigative techniques allowed Investigators to identify the identity of "Ivan BUGATZI", the **SUBJECT RESIDENCE**, the **SUBJECT VEHICLE**, and the suspected cellular phone attributable to the identity, identified as (310) 482-0611 ("TRIF's 'BUGATZI' Phone-0611"). I positively identified TRIF as the user and holder of TRIF's 'BUGATZI' Phone-0611 via subsequent court

authorization geolocation of TRIF's 'BUGATZI' Phone-0611 in conjunction with physical surveillance in November 2024 and other investigative techniques. The identification of "Ivan BUGATZI" was exclusively established by the initial identification of "Marek BALVIN" and the subsequent identification of "Karel TOKAR". This is strong evidence to indicate that the identities are intertwined and directly related to each other.

26. TRIF's fictitious identities were also supported by fraudulently created and/or altered foreign passports and other identity documents, which were frequently often used to open U.S. bank accounts and other records, including at Wells Fargo, Citibank, Bank of America, and JP Morgan Chase Bank. Most, if not all, of the bank accounts identified during the investigation were opened in and/or had money withdrawn from the account(s) in the Central District of California. Investigators have confirmed that the passports are fraudulent and the identities are fictitious; however, some of the passport numbers were legitimately issued at some point and subsequently altered. Investigators also discovered that TRIF often digitally enhanced and/or modified his self-image on the fraudulent identity documents. Thus, often the individual photograph on the passport (or other document(s)) appeared slightly different but was determined to be TRIF based on several investigative techniques, computer software, and international cooperation with Romanian authorities. For example, the altered photo would change the hair style, hair length, facial hair (i.e., mustache, beard, goatee), and the general facial characteristics (i.e., face shape, eye placement, etc.) Based on my training and experience, I know that

computer, specialized computer software, and some level of expertise is required to alter photographs. I believe TRIF did this in an attempt to elude detection by law enforcement and to obfuscate the investigation and the subsequent ability of law enforcement to identify TRIF.

27. For example, Investigators and my subsequent investigation detailed herein have identified at least 15 identities created and/or used by TRIF and likely other co-conspirators as part of TRIF's overall fraud schemes. Investigators have confirmed TRIF as the creator of these fictitious and fraudulent identities several ways, including coordination with Romanian law enforcement, the use of facial recognition and other software, seizures attributable to addresses utilized by TRIF (and other aliases), and the investigation to date. I have also reviewed numerous images used on the below documents and have determined that the individual depicted is TRIF. I am familiar with the physical attributes and appearance of TRIF by sight. The identities directly attributable to TRIF were as follows:

- Antonin LOUIS, COB: France, DOB: XX/XX/1992, PP Number XXXXX5060 (France); and,
- Sofiane MAX, COB: France, DOB: XX/XX/1992, PP Number XXXXX2440 (France); and,
- Claude GAUTHIER, COB: France, DOB: XX/XX/1990, PP Number XXXXX6367 (France); and,
- Haden GOOSSENS, COB: Belgium, DOB: XX/XX/1990, PP Number XXXX0878 (Belgium); and,
- Noah ARTHUR, COB: Belgium, DOB: XX/XX/1995, PP Number XXXX5421 (Belgium) ; and,

- Danuser BUCHER, COB: Switzerland, DOB: XX/XX/1990, PP Number XXXX9109 (Switzerland); and,
- Leon RUSU, COB: Canada, DOB: XX/XX/1990, PP Number XXXX8022 (Canada); and,
- Tiberiu ENZO – DOB: Netherlands, DOB: Unknown, PP Number XXXXK193; and,
- Axel MULLER – DOB: Germany, DOB: Unknown, PP Number XXXXXR86
- Glenn GREENFIELD – Unknown, NFI ("No Further Information")
- Aurelio ROTH – Unknown, NFI
- David HUGO, COB: Luxemburg, DOB: XX/XX/1991, PP Number XXXXV7K4 (Luxemburg); and,
- Marek BALVIN, COB: Czech Republic, DOB: XX/XX/1994, PP Number XXXX7084 (Czech Republic); and,
- Karel TOKAR, COB: Czech Republic, DOB: XX/XX/1989, PP Number XXXX5348 (Czech Republic); and,
- Ivan BUGATZI, COB: Canada, DOB: XX/XX/1991, PP Number XXXX9334, Canadian driver's license XXXXXXXXX9109.

28. Investigators have conducted physical surveillance, served administrative summons, conducted interviews, spoken with other law enforcement officers, executed court authorized searches and seizures, conducted international controlled deliveries, reviewed financial records, and various other investigative techniques as part of the ongoing investigation into TRIF and TRIF's Confidence Fraud Schemes and TRIF's fictitious and fraudulent identities.

29. My subsequent investigation has identified at least five separate financial fraud schemes committed and/or being committed by MIHAI TRIF and likely other known and unknown co-conspirators using

fictitious and fraudulently created identities between approximately March 2023 - Present, including "Marek BALVIN," and "Karel TOKAR". My investigation has also identified TRIF's "clean" fictitious and fraudulent identity that TRIF likely uses for day-to-day living. Based on my training, experience, and investigation to date, I believe that TRIF has compartmentalized his identities used in fraud schemes (i.e., "Marek BALVIN", "Karel TOKAR", and others) from his "clean" day-to-day identity (i.e., "Ivan BUGATZI") to elude detection by law enforcement. For purposes of the affidavit, I have conducted an in-depth analysis of "Marek BALVIN", "Karel TOKAR", and "Ivan BUGATZI", as detailed below.

## VI. SUMMARY OF FRAUD SCHEMES COMMITTED BY TRIF AND OTHERS

30. Based on my training and experience, the fraud schemes committed by TRIF and other unknown co-conspirators can be referred to as a Confidence Fraud Scheme. In general, a Confidence Fraud Scheme is a sophisticated plot to deceive and/or defraud individuals into giving money or other personal information to a scammer. Scammers often use a variety of methods to gain the trust of their victims, including building relationships, creating a sense of trust, and exploiting vulnerabilities.

31. In this case, TRIF and likely other unknown co-conspirators purported to be a seller(s) of a piece of heavy-duty equipment (i.e., a Kubota L39 backhoe loader tractor) or a vintage restored vehicle (i.e., a 1965 Chevrolet C-10) on a spoofed website[2] and/or on

[2] Website spoofing is a scam where cyber criminals create a website that closely resembles a trusted brand as well as a domain that is virtually identical to a brand's web domain. The goal of website spoofing is to lure a brand's customers, suppliers, partners and employees to a fraudulent website and convince them to share sensitive information like login credentials, Social Security

Facebook Marketplace[3]. Ultimately, there was no tractor or vehicle for sale and sole purpose of the scheme was to swindle victims of their money. TRIF's Confidence Fraud Scheme was then layered with other information used to deceive potential victims into believing the purported sale of the item was authentic, including the use of a spoofed and/or legitimate appearing websites (i.e., "Dennis Polk Equipment" and "S&S Auto Sales"), the use of several VoIP phone numbers[4] to communicate with the victims in various capacities (i.e., the dealerships, the shipper, etc.), the use of a shipping and other companies to coordinate the sale and/or the "transport" of the vehicle to the victim (i.e., BENSON C EQUIPMENT LLC, DP EQUIPMENT LLC, OUTLET RETAIL ONE, LLC, and STALLION CARGO AZ LLC), a use of The UPS Store Post Mailboxes (PMBs) (i.e., The UPS Store #5391 in Commerce, CA in the name of "Sofiane MAX", The UPS Store #0015 in Huntington Beach, CA and The UPS Store #0012 in Los Angeles, CA in the name of "Antonin LOUIS", The UPS Store #5626 in Sun Valley, CA in the name of "Marek BALVIN", and The UPS Store #3272 in Stevenson Ranch, CA in the name of "Karel TOKAR", and The UPS Store #4466 in Long Beach, CA in the name of "Ivan BUGATZI"), and at least four U.S.

---

numbers, credit card information or bank account numbers. Additionally, a spoofed website can also be used to give the appearance of the purported business and/or business activity to appear legitimate.

[3] Facebook Marketplace is classified-ad section of the social network that specializes in helping individuals and businesses sell items locally. Marketplace is Facebook's expansion into markets to compete with services like eBay, Craigslist, and other similar platforms.

[4] Voice over Internet Protocol (VoIP) is a technology that allows users to make phone calls and other communications over the internet instead of a traditional phone line. VoIP can be used on a variety of devices, including computers, smartphones, and VoIP phones.

financial institutions in furtherance of the fraud scheme (i.e., Bank of America, JP Morgan Chase Bank, Wells Fargo, and Citibank).[5]

32. The investigation revealed that TRIF would generally use these fraudulent and fictitious identities and related accounts for 30-90 days as part of a fraud scheme and then transition to a newly established fictitious identity once the fraud scheme was fruitful and financially benefited TRIF, i.e., a victim(s) was swindled out of money and TRIF successfully received / withdrew the funds. This constant transition and creation of new identities has made it difficult for law enforcement to proactively identity and investigate TRIF and TRIF's fraud schemes in real time. Thus, Investigators are often investigating TRIF's crimes historically, i.e., after they have already occurred and TRIF has transitioned to a new identity. Additionally, the high-quality fraudulent identity documents created and used by TRIF and TRIF's apparent knowledge base regarding the use of technology to defraud victims has also made it more difficult for law enforcement to investigate. This is evidenced by TRIF's ability to continuously and successfully open bank accounts at U.S. financial institutions and elude detection by law enforcement for more than 18 months.

## VII. VICTIM IDENTIFICATION AND INFORMATION RELATED TO TRIF AND OTHERS' CONFIDENCE FRAUD SCHEMES

33. My and other Investigators continued investigation into TRIF and TRIF's related Confidence Fraud Schemes have identified a total of 14 victims with a total loss of $351,806 in ten different states, including Alabama, California, Illinois, Kansas, Kentucky,

[5] Bank of America, JP Morgan Chase Bank, Wells Fargo, and Citibank are federally insured by the Federal Deposit Insurance Corporation (FDIC) and therefore meets the federal definition of a "financial institution" pursuant to 18 U.S.C. § 20.

Missouri, Nevada, New Jersey, North Dakota, and Oklahoma. The victims were defrauded between approximately May 2023 – September 2024.

34. As part of the investigation, Investigators and/or I have confirmed that the victims were in fact victims of TRIF's Confidence Fraud Schemes several ways. Specifically, Investigators and/or I have spoken with local law enforcement, interviewed more than 10 of the victims, interviewed at least one family member of a victim, have reviewed at least eight of the filed police reports detailing the incidents, have reviewed supporting bank records detailing the wire transfers, and conducted additional investigative follow up. Based on my training, experience, and investigation to date, I believe all identified 14 victims were victims of a Confidence Fraud Scheme perpetuated by TRIF and likely other unknown co-conspirators. I am intentionally being vague about the names and other unique identifying of the victims to protect the identities of the victims.

35. Generally, banks are obligated to refund money lost to fraud (i.e., identity theft, credit card fraud, etc.); however, banks may deny the refund if the customer was negligent or involved in the scam. Thus, in this case, all victims were at a *complete financial loss because the wire transfers were originated by the victim*. Additionally, at least two victims are currently making monthly payments on loans that were obtained to fund the wire transfers in TRIF's Confidence Fraud Scheme.

36. I have learned through the continued investigation that the losses sustained by each individual victim was substantial, including emotionally and financially. In general, a lot of the victims used their life savings and/or took out a loan to purchase an item that

would benefit themselves, their current business, and/or a new business. Often, the victims were in small towns (i.e., less than 5,000 people) and were directly and/or indirectly involved in construction, agriculture, or other employment.

37. For example, one of the victims was identified as a Captain at a local police department in the greater California area. Despite this victim's extensive police training and experience, he/she was successfully swindled out of approximately $20,000. I also identified at least two victims that had not even reported the crime because of shame and embarrassment. Based on my training and experience, I believe this is strong evidence to support my belief of TRIF's Confidence Fraud Schemes were sophisticated.

38. Specifically, between approximately March – May 2023 TRIF used the identity "Sofiane MAX" and related fictious business BENSON C EQUIPMENT LLC to open and maintain business bank accounts Bank of America Account-9289 ("BofA 'MAX' Account-9289") and JP Morgan Chase Account-8985 ("JPMC 'MAX' Account-8985"). These two accounts were used to receive funds from at least five victims out of $146,131. The funds were immediately withdrawn, spent, and/or transferred in the greater Los Angeles, CA area.

39. Between approximately March – May 2023 TRIF used the identity "Antonin LOUIS" and related fictious business DP EQUIPMENT LLC to open and maintain business bank account Citibank Account-0721 ("Citibank 'LOUIS' Account-0721"). This account was used to receive funds from at least two victims out of $43,747. The funds were immediately withdrawn, spent, and/or transferred in the greater Los Angeles, CA area.

40. Between approximately November – December 2023 TRIF used the identity "Leon RUSU" and related fictitious business OUTLET RETAIL ONE, LLC to open and maintain business bank account Bank of America Account-6936 ("BofA 'RUSU' Account-6936"). This account was used to receive funds from at least one victim out of $20,650. The funds were immediately withdrawn, spent, and/or transferred in the greater Los Angeles, CA area.

***Identification and Analysis of "Marek BALVIN"***

41. As detailed herein, the investigation identified the fictious and fraudulent identity of "Marek BALVIN" as being TRIF. The identification of "Marek BALVIN" started from a reported fraud scam that occurred in the greater Bismarck, North Dakota area using a Citibank account. HSI Bismarck subsequently initiated the investigation into fraud scam. The fraud scam was the same modus operandi as TRIF's Confidence Fraud Scams. HSI Bismarck's subsequent investigation and case coordination then overlapped with my investigation into TRIF and other known and unknown co-conspirators. HSI Vienna also assisted in the investigation because of the Czech Republic passport that identified. The investigation then expanded and identified a second bank account in the name of "Marek BALVIN" at Wells Fargo.

42. In summary, I learned that between approximately June – September 2024, TRIF used the identity "Marek BALVIN" and related fictious business STALLION CARGO AZ LLC to open and maintain business bank accounts WF 'BALVIN' Account-5272 and Citibank 'BALVIN' Account-7684. These accounts were used to receive funds from at least six victims out of $141,278, including two victims initially identified

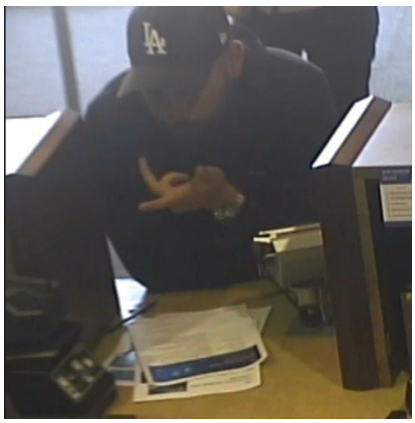
by an HSI Bismarck investigation. Both accounts were opened in August 2023 in the greater Los Angeles, CA area using the fictious identity and supporting fraudulent documents of "Marek BALVIN".

43. As shown below, I have provided still frame CCTV images from the Citibank 'BALVIN' Account-7684 showing that an individual I have identified by sight as TRIF was captured opening the account on August 22, 2024, and subsequently withdrawing funds via teller and ATM from the account on September 9, 11, 13, and 17, 2024. The fund source was from two separate victims that wired $15,000 and $16,000 on or about September 9, 2024. The two victims were identified as residing in North Dakota and New Jersey and were confirmed as victims through victim interviews by HSI Bismarck. A subsequent review of bank records for Citibank 'BALVIN' Account-7684 showed that the victim funds were immediately withdrawn by TRIF from a branch and ATM. The bank branch for all the transactions occurred at the Citibank located at 360 E Magnolia Burbank, CA 91502 ("Citibank Burbank"), which is less than 4 miles from the **SUBJECT RESIDENCE.** Additionally, a review of the ATM CCTV footage from September 17, 2024, showed TRIF arrived and departed on an e-scooter. As detailed herein, this identical scooter was later observed in the trunk of the **SUBJECT VEHICLE** on November 13, 2024, at a car wash in Arcadia, CA. The positive identification of TRIF as the sole individual that opened, maintained, and withdrew funds from the account is strong evidence to indicate TRIF's direct involvement in the Confidence Fraud Schemes.

44. An image of an individual I identified by sight as TRIF opening Citibank 'BALVIN' Account-7684 on August 22, 2024, is

depicted below. The account was opened at Citibank Burbank, which was less than 4 miles to the **SUBJECT RESIDENCE**. The image looked like this:

45. An image of an individual I identified by sight as TRIF withdrawing funds from Citibank 'BALVIN' Account-7684 on September 11, 2024, is depicted below. The funds that were withdrawn were funds from an identified victim of a Confidence Fraud Scheme. The funds were withdrawn from Citibank Burbank less than 4 miles to the **SUBJECT RESIDENCE**. It also appeared that during the transaction TRIF presented what appeared to be a passport for identification verification purposes. Based on my training and experience, I believe TRIF presented the fictious and fraudulent passport in the name of "Marek BALVIN". The image looked like this:



46. Several images of an individual I identified by sight as TRIF withdrawing funds from Citibank 'BALVIN' Account-7684 ATM in September 2024, is depicted below. The funds were withdrawn from Citibank Burbank, which was less than 4 miles to the **SUBJECT RESIDENCE**. The funds that were withdrawn were funds from an identified victim of a Confidence Fraud Scheme. In summary, TRIF arrived, withdrew funds using a card from TRIF's wallet, and subsequently departed on an e-scooter. The images looked like this:

47. As detailed herein, the identification and subsequent investigation into the fictitious and fraudulent identity of "Marek BALVIN" was the catalyst that assisted law enforcement in identifying the fictious and fraudulent identifies "Karel TOKAR" and "Ivan BUGATZI". As detailed below, the investigation confirmed that TRIF was the sole individual directly attributable to "Karel TOKAR" and "Ivan BUGATZI".

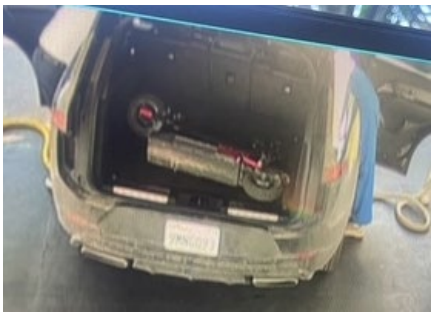
48. As part of the ongoing investigation, on November 7, 2024, United States Magistrate Judge Maria A. Audero authorized a Search and Seizure Search Warrant for prospective live tracking via GPS coordinates and historical information associated with TRIF's 'TOKAR' Phone-2154. The warrant authorized prospective live tracking via GPS

coordinates for 45 days and historical information for 30 days from the date of warrant, referencing case number 2:24-MJ-6739. The phone number was directly attributable to the fictitious and fraudulent identity of "Karel TOKAR".

49. Between approximately November – 13, 2024, I did not receive any geolocation information for TRIF's 'TOKAR' Phone-2154. Based on my training and experience, this was consistent with the phone being powered off. Then, on November 13, 2024, between approximately 9:59 a.m. PST to 5:29 p.m. PST, the phone powered on and geolocation was received in 10-minute increments. The following day, on November 14, 2024, HSI Vienna SA C. Lindsly conducted a review and analysis of the geolocation information received. As detailed below, SA Lindsly's subsequent analysis of the limited data received pursuant to the court authorized geolocation identified several locations the phone was located at, including Fasching's Car Wash, 425 N Santa Anita Ave, Arcadia, CA 91006 (Fasching's Car Wash) and a parking lot at Arcadia Mall. The geolocation information received was very accurate, including +/- 8 meters. This subsequently allowed law enforcement to collect and review CCTV footage from both locations which assisted the investigation several ways. First, a review of the CCTV footage confirmed that TRIF was the holder of TRIF's 'TOKAR' Phone-2154. Second, it identified TRIF's vehicle as the **SUBJECT VEHICLE**. Third, it identified another previously unknown alias, identified herein as "Ivan BUGATZI".

50. An image of an individual I identified by sight as TRIF and the **SUBJECT VEHICLE** on November 13, 2024, at Fasching's Car Wash is depicted below. Of note, I identified an e-scooter in the trunk of

the SUBJECT VEHICLE consistent with the e-scooter TRIF used to withdraw funds from Citibank 'BALVIN' Account-7684 in September, 2024. The image of TRIF and the **SUBJECT VEHICLE** (with the e-scooter in the trunk) looked like this:



51. Subsequent record checks revealed that TRIF's Range Rover was an Enterprise rental car rented on October 3, 2024, to "Ivan BUGATZI" and that "Ivan BUGATZI" (i.e., TRIF) is paying approximately $4,000 per month to rent TRIF's Range Rover. To date, TRIF still has an active rental agreement with Enterprise with an expected return date of November 28, 2024, according to their business records. The **SUBJECT VEHICLE** was rented using the fictitious and fraudulent identify of "Ivan BUGAZTI" and paid for using a related Bank of America account, as detailed herein. The Bank of America account and related information is detailed below. I have also reviewed a CCTV still frame on October 3, 2024, from Enterprise and confirmed that the purported renter "Ivan BUGATZI" was in fact TRIF. An image of an individual I identified by sight as TRIF and the **SUBJECT VEHICLE** departing Enterprise on October 3, 2024, is depicted below. The image looked like this:

52. The continued investigation into "Ivan BUGATZI" identified Bank of America Account number XXXXXXXXXXXX3857 ("BofA 'BUGATZI' Account-3857") and Bank of America credit card number XXXXXXXXXXXX0602 ("BofA 'BUGATZI' CC-0602") as accounts currently being used by "Ivan BUGATZI" (i.e., TRIF). Investigators have reviewed and discussed with an authorized representative the two Bank of America accounts attributable to "Ivan BUGAZTI".

53. In summary, I learned that the accounts were opened on September 17, 2024, using the fictitious and fraudulent identity and supporting documents of "Ivan BUGATZI". In general, it appears that the two accounts are being used to live lavishly with likely illicit proceeds of swindled victims using other aliases and Confidence Fraud Schemes in the greater Los Angeles, CA area, i.e., rent high-end vehicles, travel, purchase expensive jewelry, dine at restaurants, etc. The two accounts generally maintained a low account balance and would have enough funds in the account to cover general day-to-day transactions, other purchases, and to make frequent payments on BofA 'BUGATZI' CC-0602. All the funds into the accounts were cash deposits either via ATM and/or teller deposits in the greater Los Angeles, CA area. The source of the funds is unknown; however, based on my

training and experience I believe that the funds are likely proceeds of TRIF's Confidence Fraud Schemes.

54. Investigators also learned some of the purchases were as follows: UberEATS, parking, Zelle payments, purchases at various grocery stores, etc. There were also numerous payments to DDHD Jewelry in Los Angeles, CA, including $1,000 and $2,000 payments on November 18 and 19, respectively. Open-source queries revealed that DDHD Jewelry was a high-end custom jewelry store with the motto, "You Imagine It, We Bring it to Life". DDHD Jewelry also sold other jewelry, including men's rings, bracelets, women's rings, chains, earrings, pendants, etc. Based on my training, experience, and investigation to date, I believe these payments were likely for jewelry TRIF has ordered using proceeds from his known and unknown Confidence Fraud Schemes, as detailed herein.

55. Investigators also learned that TRIF's Bank of America CC-0602 also had regular day-to-day transactions, which were subsequently paid off via BofA 'BUGATZI' Account-3857. The authorized Bank of America representative stated that the activity of both accounts generally would not raise any suspicion by banking authorities. Based on my training and experience, I believe this low-risk transactional activity was conducted by TRIF purposely to elude detection by law enforcement and enable TRIF to use the identity of "Ivan BUGATZI" for day-to-day living using illicit proceeds procured from TRIF's Confidence Fraud Schemes.

## VIII. IDENTIFICATION OF THE SUBJECT RESIDENCE AND SUBJECT VEHICLE

56. As detailed herein, I am investigating TRIF for the SUBJECT OFFENSES. My investigation has spanned approximately 20 months and

has identified a sophisticated and complex fraud scheme perpetuated by TRIF and other known and unknown co-conspirators. Over the span of several months, Investigators and I have used numerous investigative techniques in an attempt to disrupt TRIF's ongoing fraud schemes. A primary objective of my ongoing investigation was to identify TRIF's primary residence, potential stash locations, and vehicles used by TRIF. As detailed below, the continued investigation has identified the **SUBJECT RESIDENCE** and the **SUBJECT VEHICLE** as TRIF's primary residence and vehicle, respectively.

57. Specifically, I have worked a historical and proactive investigation to disrupt and dismantle TRIF's Confidence Fraud Schemes and likely other fraud related activities. As detailed herein, I have identified TRIF's "clean" identity as "Ivan BUGATZI". The purpose of TRIF using "Ivan BUGATZI" is to launder illicit proceeds and to elude detection by law enforcement.

58. As detailed above, my investigation identified several Bank of America accounts attributable to "Ivan BUGATZI". A review of those accounts identified numerous transactions billed by UberEATS, including as recently as November 2024. Based on my training, experience, and opensource queries, I know that UberEATS is an online food ordering and delivery platform launched by the company Uber in 2014. The meals are delivered by couriers using various methods, including cars, scooters, bikes, or on foot. UberEATS is operational in over 6,000 cities in 45 countries as of 2021. Generally, a customer of UberEATS use an application to order food. The use of the UberEATS application requires a customer to create an account, including customer name, address, cellular phone number, payment

method(s), and other information. The provided cellular phone number is used in the event an UberEATS delivery person or the Uber driver needs to contact the intended customer. Additionally, once an UberEATS order is placed and subsequently delivered, UberEATS maintains that delivery information, including restaurant, delivery date and time, and delivery address, among other things.

59. Based in part on the aforementioned facts, on November 22, 2024, United States Magistrate Judge Alicia Rosenberg authorized a 2703(d) Court Order requesting records associated to cellular phone number TRIF's 'BUGAZTI' Phone-0611 and customer name "Ivan BUGATZI". The order authorized the requested records from the date of the account(s) inception to date of order, referencing case number 2:24-MJ-7053.

60. The following day, on or about November 23, 2024, Investigators served the Court Order via Uber Technologies, Inc's ("Uber") law enforcement portal, referencing internal Uber case number 00498516.

61. The following day, on November 24, 2024, Investigators received the records from UberEATS pursuant to the 2703(d) Court Order. The records were received via Uber's law enforcement portal.

62. On the same day HSI Vienna SA Lindsly conducted an analysis of the UberEATS records. I have spoken with SA Lindsly and conducted an independent review of the records. The records received two files, including a file titled "Response to Request – 00498516.pdf" and "Attachment to Response – 00498516.xlxs".

63. In summary the records revealed that "Ivan BUGAZTI" (i.e., TRIF) had two separate UberEATS accounts, including Display Names

"Ivan Bugatzi" and "Ivan Bug". In summary, based on a review of the records it appears that TRIF used Display Name "Ivan Bugatzi" from approximately September 29 – October 15, 2024, and Display Name "Ivan Bug" from approximately October 16 – Present, 2024. This was corroborated by a review of IP address logs, customer information, and customer order information.

64. As detailed below, a review of the records identified TRIF's primary residence as the **SUBJECT RESIDENCE**. In summary, between September 29 – November 20, 2024, TRIF (using Display Names "Ivan Bugatzi" and "Ivan Bug") had a total of 17 food deliveries. 16 of the 17 food deliveries were delivered to the **SUBJECT RESIDENCE**. The only food delivery to an alternate address occurred on September 29, 2024, and was delivered to 310 Tahiti Way #201, Marina Del Rey, CA. Additionally, I reviewed the GPS coordinates submitted by the UberEATS delivery driver, which documented the exact location the food was delivered. The delivery GPS coordinates are consistent with the **SUBJECT RESIDENCE**. The order deliveries were as follows:

| Account | Amount | Order Date / Time | Delivery Date / Time | Delivery Address |
|---|---|---|---|---|
| Ivan Bugatzi | $74.36 | 2024-09-29 12:51:49 | 2024-09-29 13:33:48 | 310 Tahiti Way |
| Ivan Bugatzi | $13.99 | 2024-10-01 9:21:22 | 2024-10-01 10:03:48 | **SUBJECT RESIDENCE** |
| Ivan Bugatzi | $41.91 | 2024-10-02 21:28:45 | 2024-10-02 22:26:00 | **SUBJECT RESIDENCE** |
| Ivan Bug | $23.92 | 2024-10-26 17:34:48 | 2024-10-26 17:48:46 | **SUBJECT RESIDENCE** |
| Ivan Bug | $39.46 | 2024-10-27 9:53:42 | 2024-10-27 10:27:46 | **SUBJECT RESIDENCE** |
| Ivan Bug | $121.45 | 2024-10-28 20:27:35 | 2024-10-28 21:21:28 | **SUBJECT RESIDENCE** |
| Ivan Bug | $32.96 | 2024-11-01 12:05:18 | 2024-11-01 12:53:20 | **SUBJECT RESIDENCE** |
| Ivan Bug | $17.98 | 2024-11-01 19:15:15 | 2024-11-01 20:00:08 | **SUBJECT RESIDENCE** |
| Ivan Bug | $81.97 | 2024-11-02 18:49:36 | 2024-11-02 19:37:52 | **SUBJECT RESIDENCE** |
| Ivan Bug | $18.96 | 2024-11-03 13:34:33 | 2024-11-03 14:10:35 | **SUBJECT RESIDENCE** |
| Ivan Bug | $61.80 | 2024-11-04 20:00:15 | 2024-11-04 20:52:35 | **SUBJECT RESIDENCE** |
| Ivan Bug | $81.97 | 2024-11-05 19:10:08 | 2024-11-05 19:53:08 | **SUBJECT RESIDENCE** |
| Ivan Bug | $25.15 | 2024-11-07 23:35:45 | 2024-11-07 23:48:54 | **SUBJECT RESIDENCE** |

| | | | | |
|---|---|---|---|---|
| Ivan Bug | $86.83 | 2024-11-15 19:28:58 | 2024-11-15 20:26:00 | **SUBJECT RESIDENCE** |
| Ivan Bug | $24.94 | 2024-11-16 16:05:31 | 2024-11-16 17:07:42 | **SUBJECT RESIDENCE** |
| Ivan Bug | $40.99 | 2024-11-19 20:09:24 | 2024-11-19 21:08:28 | **SUBJECT RESIDENCE** |
| Ivan Bug | $21.96 | 2024-11-20 23:24:55 | 2024-11-20 23:44:15 | **SUBJECT RESIDENCE** |

65. As detailed herein, Investigators and I had identified TRIF's primary vehicle as the **SUBJECT VEHICLE** and TRIF's primary residence as the **SUBJECT RESIDENCE**. On November 25, 2024, at approximately 10:45 a.m. PST, HSI SA Yoo was conducting covert physical surveillance immediately in front of the **SUBJECT RESIDENCE**. In summary, SA Yoo observed the **SUBJECT VEHICLE** pull out of a dedicated gate that gave access to the **SUBJECT RESIDENCE**. Based on SA Yoo's training and experience, it appeared that the gate was only accessible by occupants of the small complex, including the **SUBJECT RESIDENCE**, likely by an electronic remote. I also conducted a review of court authorized geolocation information obtained from TRIF's 'TOKAR' Phone-2154 and TRIF's "BUGATZI" Phone-0611. A subsequent review of the geolocation information for both phones was consistent with TRIF arriving and departing the area of the **SUBJECT RESIDENCE** consistent with SA Yoo's physical observations. Thus, this corroborates the identification of the **SUBJECT RESIDENCE** and **SUBJECT VEHICLE** as TRIF's primary residence and primary vehicle.

**TRIF Used Skimmed Debit Cards at ATMs**

66. Per video footage provided to me by Beverly Hills Police Department, TRIF utilized a Bank of America ATM in Beverly Hills, CA on February 20, 2023. Bank of America advised me that TRIF had attempted to use three stolen EDD cards and one EBT card at the same Bank of America ATM on February 20, 2023. I personally reviewed video footage of TRIF at the Bank of America ATM and confirmed his identity as the individual who attempted to use the three stolen EDD cards and

one EBT card. (To identify TRIF from surveillance images, I compared them to Romanian passport photos of MIHAI TRIF which I received from Romanian law enforcement.) Based on my training and experience, I know that criminals utilize various skimming devices and tools to steal information from EBT and EDD account holders. Criminals involved in skimming crimes often place skimming devices on ATMs and credit-card machines in order to steal the account numbers of EBT and EDD cards. Criminals then utilize other devices to create duplicate debit-cards which contain the stolen EBT and EDD victims account numbers on then. Criminals then go to ATMs and attempt to drain those victims' EBT and EDD accounts, also known as "cash-outs," as TRIF was captured on video doing. Accordingly, persons involved in skimming, like TRIF, commonly have evidence of skimming in their vehicles and residences, such as skimmers, blank cards which can be re-encoded with victims' account information, access card reader-writers, spy cameras, and related equipment.

## IX. **TRIF IS PREPARING TO CHANGE RESIDENCES**

67. While investigating the **SUBJECT RESIDENCE** online on November 26, 2024, I saw that it was advertised as being for rent. I called the listed number and pretended to be interested in renting it. In summary, I learned that the current tenant (i.e., TRIF) would be vacating it on November 29, 2024. Additionally, as detailed herein, a subsequent review of the Enterprise rental agreement showed that the **SUBJECT VEHICLE** is scheduled to be returned on November 28, 2024. Based on my training and experience, I believe it is likely that TRIF might be in the process of transitioning to a new identity. Thus, the requested warrant is time sensitive. On November 27, 2024,

I was watching the **SUBJECT RESIDENCE** and personally observed TRIF exit the residence and then enter it again in the morning.

## X. TRAINING AND EXPEREINCE ON DIGITAL DEVICES[6]

68. 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

---

[6] As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

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.

69. 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.

a) 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.

70. 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) 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 physical characteristics are among those that will unlock the device via biometric features, 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 premises without any identifying information on the exterior of the device. Thus, if while executing the warrant, law enforcement personnel encounter a digital device within the scope of the warrant that may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to, with respect to every person who is located at the TARGET PREMISES during the execution of the search who is reasonably believed by law enforcement to be a user of a biometric sensor-enabled device that falls within the scope of the warrant: (1) depress the person's thumb- and/or fingers on the device(s); and (2) hold the device(s) in front of the

face of the person with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

d) In my training and experience, Romanian TCO members often reside together to better coordinate their efforts. This is especially true for persons involved in fraud crimes as these crimes often require specialized tools and equipment to create fraudulent identification documents and the like.

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

## XI. **CONCLUSION**

72. Based upon the foregoing facts and my training and experience, I believe there is probable cause to believe that evidence of conspiracy to commit mail, wire, and bank fraud, money laundering, and passport fraud listed in Attachment B will be found at the **SUBJECT RESIDENCE** and the **SUBJECT VEHICLE.**

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this ____ day of November, 2024.

_____
UNITED STATES MAGISTRATE JUDGE