UNITED STATES DISTRICT COURT

for the

Southern District of California

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Information associated with cellular telephone number: (574)-327-1997 ("**Subject Account 2**"),

that is stored at premises controlled by T-Mobile

Case No. '23 MJ01302

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-2, incorporated herein by reference.

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

See Attachment B-2, incorporated herein by reference.

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 USC §§ 1343 and 1349	Conspiracy to Commit Wire Fraud
18 USC § 1956(h)	Conspiracy to Commit Money Laundering

The application is based on these facts:

See Attached Affidavit of FBI Special Agent Courtney M. McGuire, incorporated herein by reference.

- ☐ 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.

Courtney M. McGuire
Applicant's signature

Courtney M. McGuire, FBI 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 *(specify reliable electronic means)*.

Date: 04/11/2023

Judge's signature

City and state: San Diego, California

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

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Courtney M. McGuire, Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, hereby state as follows:

INTRODUCTION

1. I submit this affidavit in support of an application for a search warrant for **AT&T**, a wireless telephone service provider headquartered at 11760 US Highway 1, 4th floor, North Palm Beach, Florida 33408, as described in **Attachment A-1**, to search the account associated with the cellular telephone number **(562)-542-7153 (Subject Account #1),** and **T-Mobile**, a wireless telephone service provider headquartered at 4 Sylvan Way, Parsippany, New Jersey, as described in **Attachment A-2**, to search the account associated with the cellular telephone number **(574)-327-1997** (**Subject Account #2)**, altogether the "**Subject Accounts**" for subscriber information, telephone toll data, and cell-site geo-location information, for the period of July 1, 2020 up to and including and August 31, 2022. There is probable cause that these records and information constitute evidence, fruits, and instrumentalities of violations of federal criminal law, namely, Title 18, United States Code, Sections 1349 and 1956(h), as more fully described in Attachment B. This affidavit and application are sought pursuant to Rule 41 of the Federal Rules of Criminal Procedure and 18 U.S.C. § 2703(a), which applies to providers of electronic communication services. In this case, as will be shown below, AT&T and T-Mobile provide electronic communication services in the form of cellular and wireless telephone service for the **Subject Accounts**.

AGENT EXPERIENCE AND BACKGROUND

2. I am an investigative or law enforcement officer within the meaning of Title 18, United States Code, Section 2510(7); that is, an officer of the United States, who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in Title 18, United States Code, Section 2516. I have been employed as a Special Agent with the Federal Bureau of Investigation (FBI) since December of 2021. I am presently assigned to the FBI San Diego's Transnational Organized Crime – Eastern

Hemisphere (TOC-E) squad. This squad investigates wire fraud, money laundering and other derivative financial crimes committed by criminal organizations. Prior to my assignment with the TOC-E squad, I completed the 17-week FBI Academy in Quantico, Virginia and was trained in investigative techniques, procedures, and strategies. Prior to my appointment as a Special Agent, I worked for the FBI as a Tactical Specialist and administrative support employee for four years. As a Tactical Specialist, I conducted research and analyzed data in support of federal criminal and national security investigations. Prior to my appointment to the FBI, I served as a Jailer for the Laguna Beach Police Department in Laguna Beach, California. I have a Bachelor of Science degree in Biology from Boise State University.

3. As both a Tactical Specialist and a Special Agent with the FBI, I have participated in numerous investigations involving individuals of criminal organizations engaged in money laundering, drug trafficking, human trafficking and robbery. Through my investigations, my training and experience, and discussions with other law enforcement personnel, I have become familiar with the tactics and methods used by criminal enterprises to collect and launder the proceeds from specified unlawful activity to include drug trafficking, interstate transportation of stolen goods, wire fraud, and mail fraud.

FACTS SUPPORTING PROBABLE CAUSE

Background on Romanian Organized Crime Group

4. In November 2021, The San Diego Police Department (SDPD) became aware of a series of theft related crimes targeting the elderly population in San Diego. Suspects, believed to have been of Romanian descent, used force to remove money and jewelry from elderly victims or used sleight of hand techniques to remove their jewelry. Often, the suspects placed inexpensive gold colored jewelry on the victims, removing their more expensive jewelry at the same time. The suspects were consistently described as middle eastern or white subjects driving newer SUV type vehicles. Approximately 20 cases were reported to the San Diego Police Department and many more were reported throughout the county beginning in February 2020.

5. In May of 2022, SDPD and the FBI opened a joint investigation into the criminal organization responsible for the aforementioned thefts in San Diego County. The criminal organization, hereinafter the Valcea Crime Ring, was made up of Roma travelers known to conduct various frauds and thefts throughout the United States. Many of the members of the Valcea Crime Ring travel from the Valcea region of Romania to Mexico and/or Canada with the intent of entering the United States. Upon entrance into the United States, members of the organization were responsible for generating as much income as possible through theft, begging and other financial crimes.

6. On June 17, 2022, SDPD located and arrested two members of the Valcea Crime Ring, F.T. and M.C., for suspicion of money laundering and obtaining money on false pretenses. At the time of their arrest, law enforcement found a 2019 W-2 for F.T. listing Kraftsman Construction Co. as his employer. F.T. was advised of his rights, waived his rights and agreed to speak with law enforcement. F.T. stated he traveled from Romania to Toronto, Canada. On September 28, 2018, F.T. walked across the United States Canada border into New York and turned himself into United States immigration authorities. F.T. told law enforcement he bought fake jewelry and sold it as if it were real. Ultimately, F.T. and M.C. were released from SDPD custody and no charges were filed.

Identification of Constantin SANDU and Discovery of EDD Fraud Scheme

7. Following F.T.'s arrest, F.T.[1] expressed interest in providing information to law enforcement. On July 7, 2022, F.T. contacted SDPD telephonically. Investigators asked F.T. about the W-2 from Kraftsman Construction Co. found within his property at the time of his arrest. F.T. told law enforcement he did not know anything about the document and never worked for a construction company. F.T. disclosed to law enforcement he had paid a man known as "Bobi" $1,000.00 and Bobi applied for California Unemployment Insurance benefits through the Employment Development Department

[1] F.T. was not promised anything in return for his cooperation. F.T. has prior arrests for alien inadmissibility and driving without a license. Additionally, as of March 28, 2023 F.T. had an active arrest warrant out of Georgia for a failure to appear in May of 2022.

(EDD) on behalf of F.T. After the phone call with law enforcement, F.T. sent Investigators a picture of Bobi's Facebook account with the display name of Bobi Constantin and username fabritio.constantin. Investigators reviewed Bobi's Facebook profile and observed numerous pictures of the individual F.T. identified as Bobi.

8. On July 26, 2022, Investigators obtained authorization from the Superior Court of the State of California (SW#2207261250-SDPD-MDK-SW) for Meta Platforms, Inc. to provide information associated with the "Bobi Constantin" Facebook profile. Investigators compared photographs posted to the profile with photographs of an individual already under investigation for COVID-19 fraud named Constantin SANDU. They determined that SANDU was the same person as the Facebook profile "Bobi Constantin."

9. Investigators reviewed data obtained from Facebook associated to SANDU's Facebook profile "Bobi Constantin". A review of Facebook posts and messages revealed SANDU had spoken to more than 75 different individuals about obtaining EDD benefits. In those conversations, the individuals provided SANDU with personal identifiable information (PII) including names, dates of birth, identifications, and social security numbers[2] (SSNs) for themselves and their family members. SANDU replied with e-mail addresses, passwords, and tax documents, including W-2s, bearing the shared PII.

10. On or around June 2022, Detectives contacted EDD investigators and obtained account information for accounts associated with the PII identified in SANDU's Facebook messages. EDD identified more than 100 accounts relating to those persons, who collectively obtained more than 8 million dollars in EDD benefits beginning in July of 2020. In the majority of the applications submitted, individuals claimed to be United States citizens, assumed an SSN not assigned to them, and uploaded fraudulent supporting documents to include fake identifications, utility bills, and health insurance cards. According to Department of Homeland Security, the majority of the applicants were not

[2] In my training and experience, I know that a Social Security Number (SSN) is a nine-digit, unique identifier issued by the Social Security Administration to U.S. citizens, permanent residents, and temporary (working) residents. It is needed to work and is used to determine an individual's eligibility for Social Security benefits and certain government services. Most individuals have only one SSN.

United States Citizens. According to the Social Security Administration, the majority of applicants used SSNs that were non-existent or assigned to other individuals. Additionally, based on records from Departments of Motor Vehicles (DMVs), Anthem Blue Cross, and Southern California Edison, the majority of the supporting documents provided by these applicants were not valid. Applicants submitted the documents they had received from SANDU as proof of their eligibility for benefits.

Background on California EDD

11. The Unemployment Insurance ("UI") Program is a joint federal-state partnership administered on behalf of the U.S. Department of Labor by agencies in each state. In the State of California, the UI Program is administered by California's Employment Development Department ("California EDD").

12. On March 13, 2020, President Trump declared a nationwide emergency due to COVID-19, and in March 2020, the Families First Coronavirus Response Act (FFCRA) and the Coronavirus Aid, Relief, and Economic Security (CARES) Act provided additional funding for state UI agencies to respond to the COVID-19 pandemic. The CARES Act allowed states to expand the scope of workers who were eligible to receive state UI benefits, to extend the period of time for which workers could be eligible for UI benefits, and to allow workers who may have exhausted UI benefits under traditional programs to receive benefits.

13. The CARES Act further expanded the ability of states to provide benefits to unemployed workers by creating three new unemployment programs, namely, the Pandemic Unemployment Assistance (PUA) program, which permitted states to provide benefits to individuals who were self-employed, seeking part-time employment, or otherwise would not qualify for regular unemployment benefits, the Federal Pandemic Unemployment Compensation (FPUC) Program, which provided an additional amount in federal benefits to individuals collecting traditional UI program benefits, and the Pandemic Emergency Unemployment Compensation (PEUC) program, which provided additional weeks of benefits for individuals who had otherwise exhausted their entitlement to regular

UI benefits (collectively referred to herein as "expanded pandemic UI benefits") PUA and FPUC benefits were 100% federally funded benefits paid through state UI agencies. To receive UI, PUA, PEUC, and FPUC benefits from a state UI agency, an applicant could file a claim, via the internet, with the state UI agency from which he was eligible to seek benefits.

14. California EDD provided unemployment insurance benefits for regular UI and expanded UI pandemic benefits to individuals whom California EDD determined were entitled to receive such benefits through debit cards, which were funded by California EDD and issued by Bank of America N.A.

15. California EDD's determination of whether the individuals were entitled to receive unemployment insurance benefits relied, in part, on confirmations from the employer (from which the individual has been recently unemployed) that the employee had worked with the employer.

16. Once a debit card for unemployment insurance benefits was issued, California EDD funded those debit cards by having funds drawn from the United States federal treasury in Washington, D.C., and wired those funds to Bank of America N.A.

17. Bank of America N.A. utilized debit processing services located in Colorado and Virginia to create accounts, load funds, and post payments for unemployment insurance debit cards. When a withdrawal was made from an account using a debit card, information was sent electronically to servers in Colorado and Virginia to post a debit to the account.

18. Between March and October 2020, over 8 million Californians filed for unemployment benefits. In light of the high volume of applications, on October 5, 2020, California implemented a new verification process for EDD through ID.me, which provided an automated process with a virtual in-person session with an ID.me representative, known as a "trusted referee," to quickly verify the identity of the applicant through a multi-step process using Artificial Intelligence and Human Intelligence together.

19. With the addition of ID.me, each applicant needed to complete a verification process before applying for benefits. Once the verification process was completed, they could re-enter the EDD portal and apply for benefits. The applicant would be given a "Confirmation Number" associated to their application for future reference.

20. Once approved for pandemic benefits, the recipient of the benefits would be required to periodically recertify under the penalties of perjury that, among other things, the recipient was unemployed due to the COVID-19 pandemic and therefore remained eligible to receive pandemic benefits.

Identification of David CONSTANTIN as Major Participant in the Fraud

21. Within the Facebook returns for SANDU, SDPD investigators located a conversation with an account bearing the name "David Dzl", user account 100004263034314. Using the photographs contained on the profile, investigators were able to identify the user of Facebook account "David Dzl" as David CONSTANTIN by comparing them to the photograph of CONSTANTIN on a Washington driver's license.

22. On February 27, 2023, SANDU, along with his wife and four children, was encountered by Border Patrol entering the United States illegally, approximately one mile west of the San Ysidro, California Port of Entry and approximately 100 yards north of the United States/Mexico International Boundary. Sandu was detained by Border Patrol and then arrested by the FBI on March 1, 2023. On March 1, 2023, SANDU agreed to waive his rights and speak to investigators. Among other things, he admitted to applying for EDD benefits, assisting family in applying for EDD benefits, and sending approximately $24,000.00 to a contractor in Romania to renovate his house. SANDU further admitted that he used a friend to obtain fraudulent W-2s, false identifications, fraudulent utility bills and fraudulent insurance cards for the purposes of applying for EDD benefits. SANDU told law enforcement David CONSTANTIN was his brother and identified CONSTANTIN as the user of the Facebook account "David Dzl". SANDU is currently pending prosecution in the Southern District of California, Case No. 23-CR-0386-LAB. He has expressed a desire to cooperate with law enforcement.

23. In the Facebook conversation between SANDU and CONSTANTIN, Investigators observed SANDU frequently forward the PII he received from other individuals to CONSTANTIN. CONSTANTIN frequently replied to SANDU a short time later with tax documents bearing the PII. Investigators identified over 100 people for whom CONSTANTIN provided SANDU tax documents, frequently W-2s. Investigators identified many similarities between the documents, including common businesses, common formatting, and common amount of reported yearly earnings. Based on records from the California Franchise Tax Board, Southern California Edison, and Anthem Blue Cross, the W-2s, utility bills and insurance cards submitted in support of these EDD applications were falsified. The following are examples of Facebook message conversations between SANDU and CONSTANTIN about EDD:

a. On July 29, 2021, co-conspirator F.M. sent SANDU an EDD email via Facebook message showing the confirmation of a new online account for F.M. Additionally, on July 29, 2021, SANDU sent CONSTANTIN via Facebook message the email address that was later used for A.V. and F.M.'s EDD applications.

b. On July 17, 2021, SANDU sent co-conspirator N.M. email address namoln67@gmail.com via Facebook message. This email address was originally sent to SANDU via Facebook message by CONSTANTIN.

c. On July 14, 2021, co-conspirator I.C.A. and SANDU coordinated via Facebook message about EDD. SANDU sent two photographs of the EDD portal security question screen for an account associated to email address combic757@gmail.com. This email was associated to I.C.A.'s EDD application and separately shared between SANDU and CONSTANTIN via Facebook message.

d. On August 14, 2021, co-conspirator S.G. and SANDU coordinated via Facebook message about EDD. The same day, CONSTANTIN sent

SANDU via Facebook message two falsified documents for S.G. including a W-2 and Southern California Edison utility bill.

24. On April 6, 2023, SANDU and his attorney met with Investigators and federal prosecutors. SANDU was not promised anything in exchange for his cooperation. During his proffer, SANDU explained that he and CONSTANTIN learned from a friend how to create fraudulent documents and submit EDD applications. After a short time, SANDU and CONSTANTIN went into business on their own. SANDU told law enforcement CONSTANTIN assisted with creating the fraudulent documents required to submit EDD applications. According to SANDU's statements, CONSTANTIN and SANDU maintained versions of W-2s, Southern California Edison utility bills and health insurance cards. SANDU told law enforcement he and CONSTANTIN would just change the name, address and SSN on the documents. These statements corroborated investigators understanding of the scheme based on their own review and investigation.

25. Based on a review of SANDU's Facebook messages and ID.me[3] verification videos, investigators determined SANDU and CONSTANTIN frequently met with co-conspirators at parks to submit EDD applications and conduct ID.me verification videos. Investigators believe SANDU and CONSTANTIN assisted co-conspirators through ID.me verification videos. On the following occasions, CONSTANTIN was present for a co-conspirator's verification session:

a. On or about July 9, 2021, CONSTANTIN and SANDU were identified by law enforcement in the background of co-conspirator, R.D.'s, ID.me verification session.

b. On or about August 4, 2021, CONSTANTIN was identified by law enforcement assisting co-conspirator, M.A., throughout their ID.me verification session.

[3] On October 5, 2020, California implemented a new identity verification process for EDD by contracting with a third party company, ID.me. EDD applicants were required to submit their supporting documentation to ID.me. Once the documents were reviewed, the applicant would conduct an ID.me verification video session with an ID.me representative, known as a "trusted referee".

Money Obtained Through Wire Fraud and Conspiracy to Commit Wire Fraud

26. Investigators reviewed the records obtained from EDD, ID.me and Facebook, including records associated with CONSTANTIN and Maria ALEXANDRU (identified as CONSTANTIN's wife). CONSTANTIN and ALEXANDRU applied for EDD benefits on multiple occasions. On July 6, 2021, CONSTANTIN applied for EDD benefits using a fraudulent W-2 listing Bless Tires & Auto Repair as his employer. CONSTANTIN listed his telephone number as **(562)-542-7153** (**Subject Account #1**) on his July 6, 2021 EDD application.

27. On July 11, 2021, ALEXANDRU applied for EDD benefits using a fraudulent W-2 listing TLC Cleaning as her employer. According to the California Franchise Tax Board, Bless Tires & Auto Repair and TLC Cleaning were not legitimate companies registered in the state of California. Despite this, both fraudulent W-2s documented the payment of California state tax under a non-existent state tax identification number. Investigators determined CONSTANTIN applied for EDD benefits on another occasion under the alias Vlad Alexandru using another W-2 identifying Bless Tire & Auto Repair as his employer. Additionally, investigators determined ALEXANDRU applied for EDD benefits on another occasion under the alias Cristina Constantin using another W-2 identifying TLC Cleaning as her employer. From these fraudulent applications, CONSTANTIN and ALEXANDRU obtained over $110,000.00 in EDD benefits.

28. CONSTANTIN listed telephone number **(574)-327-1997** (**Subject Account #2)** on his July 29, 2021 EDD application submitted under the alias Vlad Alexandru. Investigators reviewed the ID.me verification video and selfie photographs submitted in support of Vlad Alexandru's EDD application. Based on the comparison of CONSTANTIN's Washington driver's license, investigators identified CONSTANTIN to be the true identity of Vlad Alexandru. Additionally, a review of SANDU's historical call detail records (received pursuant to a warrant authorized by U.S. Magistrate Judge Barbara L. Major, No. 23MJ1164-BLM) revealed contact with **Subject Account #1** and **Subject Account #2** during the course of the fraud scheme.

29. Based on SANDU's statements during the proffer interview, SANDU and DAVID charged approximately $2,500.00 to assist others in filing applications. SANDU told investigators they charged $1,000.00 up front and $1,500.00 once the individuals received their money, but not everyone would pay.

30. On July 17, 2021 in a publicly viewable Facebook post by CONSTANTIN, CONSTANTIN marketed their EDD application business. Based on a google translation, the post read "you want EDD account $1000.00 now". During SANDU's proffer interview, SANDU reviewed this post and told law enforcement it described their marketed payment plan of $1,000.00 now and $1,500.00 after the EDD payout.

31. SANDU's statements to Investigators on April 6, 2023 are corroborated by a review of Facebook messages between SANDU and co-conspirators. SANDU charged a fee assisting individuals with submitting fraudulent EDD applications online. Based on Facebook messages, SANDU received payment for his services via counter deposit[4] and Zelle transfers. On multiple occasions via Facebook message, SANDU sent his Bank of America account and routing numbers to co-conspirators to conduct counter deposits into SANDU's bank account following an EDD payout. The following are examples of SANDU's means and methods for receiving funds obtained via EDD fraud from his co-conspirators.

a. I.C. communicated directly with SANDU via Facebook message regarding EDD applications for himself and his wife, L.D. On July 10, 2021, L.D. fraudulently applied for EDD, and ultimately received $27,000.00. On September 2, 2020, SANDU sent his account and routing information to I.C. via Facebook message. I.C. responded to SANDU via Facebook message with a receipt for a $300.00 deposit. According to SANDU's bank account records, a $300.00 counter deposit was conducted on September 2, 2020.

[4] A counter deposit is referred to as a financial transaction at a bank branch in which an individual deposits money in person into a bank account.

b. On September 2, 2020, F.R. applied online for EDD benefits. F.R. received his/her first EDD payment on October 23, 2020 and received a large payment on November 4, 2020. A few days after the large payment, on November 11, 2020, SANDU sent F.R. his account and routing information. The following day, a $250 transfer was made into SANDU's account.

c. C.S. communicated directly with SANDU via Facebook message about EDD for himself and his wife, R.M. On July 31, 2020, C.S. applied online for EDD benefits. On December 26, 2020, R.M. applied online for EDD benefits. C.S. received an EDD payout on August 7, 2020 and R.M. received an EDD payout on December 30, 2020. On December 10, 2020, SANDU sent C.S his account and routing information via Facebook message. C.S. responded the same day with a photo of a Bank of America receipt confirming a $900.00 deposit. According to records for SANDU's bank account, a $900.00 counter deposit was conducted on December 10, 2020.

d. R.D. communicated directly with SANDU via Facebook message regarding EDD fraud on behalf of himself and four other individuals: M.D., A.M., A.D., and M.C.. In July 2021, three of the individuals fraudulently applied for and received EDD benefits. On September 29, 2021, M.C. received the group's final EDD payout. On the same day, R.D. sent SANDU five $500.00 Zelle transfers.

32. Investigators believe CONSTANTIN received a portion of the criminally derived funds based on the flow of funds from SANDU to CONSTANTIN during the period of the fraud scheme. Between December 2020 and August 2022, SANDU sent $16,747.00 via 37 different Zelle transfers to a Zelle account in the name of CONSTANTIN. Additionally, during SANDU's proffer interview, SANDU told law

enforcement he gave CONSTANTIN between $400.00 and $1,000.00 per EDD application.

33. A review of SANDU's bank account showed SANDU had used the online money transfer service Remitly[5] to transfer large amounts of money to an individual in Romania during the period of the fraud scheme. According to records received from Remitly, between May 19, 2021 and August 14, 2022, SANDU sent 20 transactions totaling more than $16,000.00 for the purposes of SANDU's home renovations in Romania. SANDU's post-arrest interview on March 1, 2023, confirmed his intentions of sending money to Romania for the purposes of renovating his house.

34. During the April 6, 2023 proffer, SANDU told law enforcement CONSTANTIN also sent money to Romania throughout the course of the fraud scheme for the purposes of renovating CONSTANTIN's house in Pitesti, Romania.

SANDU and CONSTANTIN's Use of Cellular Telephones Throughout Their Conspiracy

35. A review of ID.me records identified four devices with specific device fingerprints[6] that were used to create and/or modify ID.me profiles that facilitated the verification of at least 137 fraudulent EDD applications for 137 different individuals. Investigators traced each of the four devices to SANDU and/or CONSTANTIN through conversations and EDD applications they created.

36. This is consistent with SANDU's statements during the proffer interview. SANDU told law enforcement he and CONSTANTIN met with co-conspirators at parks to submit EDD applications and conduct ID.me verification sessions on their cellular telephones. SANDU disclosed that he and CONSTANTIN used many cellular telephone

[5] Open source research identified Remitly as a financial institution known for sending money abroad. As of March 28, 2023, Remitly marketed their business as "Remit Money Abroad – Remit Quickly". Based on my training and experience, individuals who have obtained money fraudulently, through illicit means and/or otherwise specified unlawful activity will often attempt to repatriate those funds to another country for the purposes of concealing the source and nature of the funds or to further promote specified unlawful activity.

[6] A device fingerprint is a unique identifier (aggregated hash value) associated with a user's device, from the hardware, operating system, audio stack, and its configuration. Browser fingerprinting refers to the process of collecting information through java script to create a fingerprint of a device.

numbers throughout their conspiracy as they would purchase a cellular device from a private retailer and obtain SIM cards from a wireless cellular telephone service company, like AT&T. SANDU told law enforcement he and CONSTANTIN telephonically contacted EDD on numerous occasions. A review of SANDU's call detail records revealed hundreds of contacts with telephone numbers associated to EDD during the period of July 1, 2020 to August 31, 2022.

METHODOLOGY

37. Based on the facts above, there is reason to believe that CONSTANTIN committed illegal activities, and that CONSTANTIN used the **Subject Accounts** to communicate with SANDU and others for the purpose of conspiracy to commit wire fraud and money laundering. I believe that the **Subject Accounts** will produce evidence that provides further corroboration of these.

38. Based on my training and experience, and my consultation with other law enforcement officers, I am aware that AT&T and T-Mobile routinely collect and store data for the electronic communication accounts to which it and other providers issue telephone numbers. The data includes: (i) subscribers' contact and billing information; (ii) detailed information concerning subscribers' incoming and outgoing telephone calls; (iii) detailed information concerning subscribers' outgoing direct calls, text message, and SMS messages; and (iv) detailed information concerning cell-site geo-location data.

39. In particular, I know that cell phones connect to a provider's network through cell towers or cell sites. The particular tower or site may change as a phone moves from one location to another. Providers automatically record and retain this connection data as part of the account. Records and data identifying the towers or sites to which a phone connected therefore tend to identify the phone's and phone user's location at particular times.

40. Given these facts, I seek a warrant to search the **Subject Accounts** for the records and information in Attachments B-1 and B-2.

PRIOR ATTEMPTS TO OBTAIN THIS EVIDENCE

41. The United States is unaware at this time of other attempts by the U.S. government to obtain this data by other means.

I swear the foregoing is true and correct to the best of my knowledge and belief.

Courtney M. McGuire

Courtney M. McGuire
Special Agent, FBI

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 11th day of April 2023.

HONORABLE MICHAEL S. BERG
United States Magistrate Judge

ATTACHMENT A-2
PROPERTY TO BE SEARCHED

T-Mobile hosts the electronic communication account associated with the telephone number **(574)-327-1997 (Subject Account #2)** that is the subject of this search warrant and search warrant application. **T-Mobile** is an electronic communication service provider whose primary computer information systems and other electronic communications and storage systems, records, and data are located at 4 Sylvan Way, Parsippany, New Jersey.

ATTACHMENT B-2
ITEMS TO BE SEIZED

I. Service of Warrant

The officer executing the warrant shall permit the Provider in **Attachment A-2,** as custodian of the electronic files described in Section II below, to locate the files and copy them onto removable electronic storage media and deliver the same to the officer.

II. Items to Be Seized

Agents shall seize the following records, data, and information covering July 1, 2020 up to and including and August 31, 2022 and maintained by the Provider for **Subject Account #2** identified in **Attachment A-2**:

a. Subscriber information, including:
   i. Names;
   ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
   iii. Local and long distance telephone connection records;
   iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
   v. Length of service (including start date) and types of service utilized;
   vi. Telephone or instrument numbers, including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");
   vii. Other subscriber numbers or identities; and
   viii. Means and source of payment (including any credit card or bank account number) and billing records.

b. Records and other information about past wire or electronic communications sent or received by the subject account, including:
   i. the date and time of the communication;
   ii. the method of the communication;
   iii. the source and destination of the communication, such as the source and destination telephone numbers (call detail records), email addresses, or IP addresses; [and]

iv. Cell site locations and sectors for all outgoing and incoming voice, SMS, MMS, and Data communications;

Which are evidence of violations of Title 18, United States Code, Sections 1349 and 1956(h).

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by **T-Mobile**, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of **T-Mobile**. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of **T-Mobile,** and they were made by **T-Mobile** as a regular practice; and

b. such records were generated by **T-Mobile's** electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of **T-Mobile** in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by **T-Mobile**, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature