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)
Apple iPhone, IMEI 356715110833004
("Target Device")

Case No. **23MJ1154**

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, incorporated herein by reference.

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

See Attachment B, 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*
Title 18 U.S.C. Section 1349	Conspiracy to Commit Wire Fraud
Title 18 U.S.C. Section 1956(h)	Conspiracy to Commit Money Laundering

The application is based on these facts:

See Attached Affidavit, 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: March 30, 2023

Barbara L. Major
Judge's signature

City and state: San Diego, California

Barbara L. Major
Hon. , United States 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 make this affidavit in support of an application for a search warrant to search the following electronic devices, as described in Attachment A, and seize evidence of crimes, specifically, violations of Title 18, United States Code, Sections 1349 and 1956(h), as more particularly described in Attachment B:

a. Apple iPhone, IMEI 356715110833004 **(Target Device).**

This search supports an investigation conducted by the FBI into **Constantin Bobi SANDU** who is suspected of committing one or more of the crimes mentioned above. A factual explanation supporting probable cause follows.

2. The **Target Device** was one of four cell phones along with an envelope of cash seized following the arrest of SANDU for wire fraud conspiracy on March 1, 2023. SANDU identified one of the phones, **Target Device**, as his own cell phone. SANDU is currently pending charges in the Southern District of California in Case No. 23-CR-0386-LAB. The **Target Device** is currently in the possession of the San Diego Police Department at 1401 Broadway, San Diego, CA 92101.

3. Based on the information below, there is probable cause to believe that a search of the **Target Device** will produce evidence of the aforementioned crimes, as described in Attachment B.

4. The information set forth in this affidavit is based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, my review of documents and computer records related to this investigation, communications

with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of obtaining a search warrant for the **Target Device**, it does not set forth each and every fact that I or others have learned during the course of this investigation, but only contains those facts believed to be necessary to establish probable cause.

EXPERIENCE AND TRAINING

5. 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 – Global squad (TOC-G). This squad investigates money laundering and other derivative financial crimes committed by criminal organizations. Prior to my assignment with the TOC-G 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.

6. 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 IN SUPPORT OF PROBABLE CAUSE

7. Based on the facts of this case, I believe that evidence of wire fraud and money laundering conspiracies may be found on the **Target Device**. Additionally, the search of the **Target Device** may also identify other individuals engaged in these crimes.

Background on Romanian Organized Crime Group

8. In September 2021, Romanian law enforcement provided information to the FBI regarding various organized crime groups coming to the United States from Romania to commit various frauds, swindles, and schemes, to obtain as much money as possible and then launder the funds back to Romania. In November 2021, the San Diego Police Department (SDPD) became aware of a series of felony theft related crimes targeting the elderly population in San Diego, believed to have been committed by Romanian organized crime groups.

9. Through a series of custodial interviews and search warrants for Facebook accounts used by members of the Romanian organized crime groups, investigators discovered a separate but overlapping wide-spread conspiracy to conduct wire fraud and fraudulently obtain unemployment benefits in California. This conspiracy was perpetrated by hundreds of members of Romanian organized crime groups, and was facilitated by SANDU.

Background on California EDD

10. 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").

11. 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.

12. 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.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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.

18. 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" connected to their application for future reference.

19. 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.

SANDU's Role In The Wire Fraud Conspiracy

20. Based on an interview with a cooperating witness, and the review of social media search warrant returns, EDD applications and ID.me records, Investigators determined that SANDU developed a process to receive the most benefits possible by using fraudulent identifications, falsified utility bills, falsified earnings statements, falsified W2s, and fraudulent Health Insurance cards. He would also "backdate" or modify an EDD application with an earlier unemployment start date to generate additional fraudulent income.

21. In June 2022, cooperating witness F.T.[1] identified SANDU via his Facebook profile as the individual who assisted with F.T.'s fraudulent EDD application. Facebook returns associated with SANDU later confirmed for Investigators that SANDU had conspiratorial conversations on Facebook with individuals looking to fraudulently apply for EDD benefits or "backdate" their EDD applications.

22. SANDU applied for EDD four separate times, on September 18, 2020, July 10, 2021, July 13, 2021, and June 5, 2022. For the application submitted on September 18, 2020, which was submitted prior to the implementation of the ID.me verification process, SANDU received $3,600.00. On this application,

[1] F,T. was detained in June of 2022 for suspicion of California Penal Code (PC) 186.10 (a) money laundering, PC 182(a)(1) conspiracy and PC 532(a) obtain money under false pretenses. F.T. waived his/her Miranda rights and provided a voluntary statement to law enforcement. F.T. was not promised anything in return for his/her cooperation and was ultimately released. 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.

SANDU listed his true social security number (SSN). SANDU used different, and fraudulent[2], SSNs in each subsequent application.

23. In the application submitted on July 10, 2021, SANDU submitted a photograph of himself, a Maryland ID, and a W-2 showing he worked for Kraftsman Construction Co. According to California Franchise Tax Board records, Kraftsman Construction Co. does not exist. Despite this, SANDU's W-2 indicates payment of California State income tax using a fraudulent California State Identification Number for Kraftsman Construction Co. In support of this fraudulent application, SANDU participated in an ID.me verification session where he confirmed he was applying for California EDD benefits. SANDU received $24,600.00 for this application.

24. In the application submitted on July 13, 2021, which SANDU submitted under the alias Ionut Mihai, SANDU submitted a photograph of himself, a Washington state ID, a California state ID, and another W-2 from Kraftsman Construction Co. Investigators compared the supporting documents and photographs for "Ionut Mihai's" application to confirm the applicant's true identity to be SANDU. Additionally, SANDU participated in an ID.me verification session where he confirmed he was applying for California EDD benefits and received $26,250.00 for this application. In the application submitted on June 5, 2022, SANDU again used a different SSN, submitted another W-2 from Kraftsman Construction Co., and a Maryland ID. He did not receive benefits from this application.

[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.

25. Beginning in July 2021, SANDU and another individual sent public announcements via social media to a large network of co-conspirators, offering services or meetings to conduct the fraud. Co-conspirators communicated with SANDU via Facebook messaging or other electronic means, and/or met with him in person to provide their personal identifying information (PII). SANDU used PII provided by co-conspirators to create or have others create the fraudulent documents listed above, which SANDU then submitted in support of fraudulent EDD applications.

26. Beginning in October 2020, EDD contracted with ID.me to assist in the identity verification of applicants. ID.me developed a process to verify supporting documents submitted by EDD applicants. As a result, applicants were required to participate in a recorded ID.me video verification session. Investigators reviewed many EDD applications using the ID.me verification process. A review of ID.me records identified four devices with specific device fingerprints[3] 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 his assistant through conversations and EDD applications they created. Investigators also reviewed hundreds of ID.me verification sessions for SANDU's co-conspirators. On several occasions, SANDU and his assistant, were seen in the background of recorded ID.me video sessions for various co-conspirator EDD applications.

27. Hundreds of EDD applications were reviewed by Investigators. They identified a significant number of consistencies across numerous supporting documents provided by applicants that reflected SANDU's reuse of resources in

[3] 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.

support of the scheme. For example, documents submitted in support of co-conspirators' applications listed the same names of businesses, Employer Identification Numbers (EINs), California State Identification Numbers, Blue Cross/Blue Shield member identification numbers, account numbers for Southern California Edison utility bills and passwords ("Romania221$") for almost all email addresses used to submit EDD applications. According to the California Franchise Tax Board, none of the companies in the various W-2's submitted for conspirators' EDD applications were established companies in the State of California. Despite this, all W-2's submitted for conspirators' EDD applications indicate California State Income Tax withholdings by companies with fraudulent California State Identification Numbers. According to Blue Cross/Blue Shield and Southern California Edison, none of the member identification numbers or account numbers submitted in support of co-conspirators EDD applications were real.

28. In total, SANDU is believed to have conspired with at least 214 unnamed co-conspirators to fraudulently obtain no less than $5,207,687.00 in California Unemployment Insurance benefits. For his services, Investigators have determined that SANDU was then paid a fee by the individual co-conspirator, often ranging between $250.00 and $1,000.00.

a. For example, social media returns showed that on July 14, 2021, A.G. communicated with SANDU via Facebook regarding EDD for his wife, T.G. On July 14, 2021, T.G. participated in a recorded video interview with ID.me, in which she identified herself by name and date of birth, and confirmed that she was applying for California EDD. A fraudulent Anthem Blue Cross/Blue Shield member ID was added to her ID.me account. On July 15, 2021, A.G. sent SANDU a Facebook message with the phone number 669-239-5640. Following this, SANDU sent A.G. a screenshot via Facebook message of an

EDD application confirmation screen for T.G. with confirmation number 38022946. SANDU also sent A.G. via Facebook message the email address marta22121m@gmail.com and the password Romania221$. Also on July 15, 2021, SANDU received via Facebook message a falsified W-2 for T.G. from another individual. According to California Franchise Tax Board, the company listed does not exist in the State of California.

b. According to EDD records, an application was submitted for T.G. on July 15, 2021, under the email address of marta22121m@gmail.com. The phone number connected to the application was 669-239-5640, the same as the number provided by A.G via Facebook message.

c. On July 25, 2021, T.G. began receiving EDD benefits, ultimately totaling $27,000.00.

d. In October 2021, A.G. told SANDU he would be in San Diego, and they discussed money. Bank of America records show the money fraudulently obtained by A.G. and T.G. was withdrawn at ATMs in the Southern District of California, as well as in Oregon and other parts of California, including a $400.00 ATM withdrawal in Escondido, CA on August 4, 2021. Specifically, Bank of America ATM footage revealed A.G. withdrawing money from T.G.'s EDD account in California both by himself and with T.G.

e. In another example, on July 14, 2021, C.G. participated in a recorded video interview with ID.me, during which he confirmed that he was applying for California EDD benefits, and presented a fraudulent California driver's license. According to the California DMV, this drivers license number belongs to someone else. On July 15, 2021, SANDU sent C.G. a Facebook message indicating that he "needed a

W-2". That same day, C.G. responded with a W-2 for his son, providing a SSN and photograph with the email address gioninebunuo@gmail.com, the password Romania221$, and the phone number 714-837-3249. An application for unemployment benefits was submitted to EDD for this individual, claiming to be a US Citizen, and being employed by Kraftsman Construction, on the same day.

f. SANDU sent the ID.me verification codes for both C.G. and his son to C.G., and on July 15, 2021 sent a facebook message to C.G. with a confirmation screen from EDD, confirmation number 38029477. On August 9, 2021, C.G.'s son began receiving $6,000.00 in EDD benefits. On August 29, 2021, C.G. began receiving $27,000.00 in EDD benefits.

g. Bank of America records confirm C.G. withdrew $26,950 from ATMs in the Southern District of California, including $900 in Escondido, CA on September 23, 2021, as well as other parts of California. As of December 29, 2022, the account had a balance of $8.27.

29. Ultimately, Investigators have determined, based on cooperating witness interviews, financial records, social media search warrant returns, and the review of EDD applications and ID.me records, that between September 2020 and August 2022, SANDU conspired with over 214 individuals known and unknown to commit this wire fraud.

SANDU's Laundering of the Money Obtained

30. According to a review of Facebook messages between SANDU and co-conspirators, SANDU charged a fee between $250.00 and $1,000.00 for 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.

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,

[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.

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.

31. A review of records associated with SANDU's Bank of America account revealed numerous payments to a Remitly account[5]. Separately, a review of SANDU's Facebook messages revealed conversations with I.T. regarding construction work on a house in Romania. I.T. sent SANDU numerous photos of a house in Romania, construction materials, invoices, and receipts from a Romanian home supply store. In response to the receipts, and invoices, SANDU responded with a screenshot of a Remitly transfer confirmation showing funds were sent from SANDU to I.T. According to records received from Remitly, between May 19, 2021 and August 14, 2022, SANDU sent 20 transactions to I.T. totaling more than $16,000.00. In September 2022, Investigators learned SANDU returned to Romania. On October 25, 2022 and December 6, 2022, SANDU posted

[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.

photos of himself and his family members in the vicinity of the aforementioned house in Romania. Additionally, Facebook comments indicated the house was owned or occupied by SANDU.

SANDU's Statement of the Offense and Criminal Proceedings

32. 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, he 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. Additionally, SANDU identified the **Target Device** as being his cellular phone.

33. On March 2, 2023, a federal complaint was filed in the Southern District of California charging SANDU with Conspiracy to Commit Wire Fraud, in violation of 18 U.S.C. § 1349. On March 28, 2023, SANDU was arraigned on an information charging him with Conspiracy to Commit Wire Fraud, in violation of 18 U.S.C. § 1349 and Conspiracy to Launder Monetary Instruments, in violation of 18 U.S.C. § 1956(h). He is currently pending those charges in Case No. 23-CR-0386-LAB.

METHODOLOGY

34. It is not possible to determine, merely by knowing the mobile electronic device's make, model and serial number, the nature and types of services

to which the device is subscribed and the nature of the data stored on the device. Mobile electronic devices, including cellular telephones and tablets, can be simple cellular telephones and text message devices, can include cameras, can serve as personal digital assistants and have functions such as calendars and full address books and can be mini-computers allowing for electronic mail services, web services and rudimentary word processing. An increasing number of cellular service providers and installable software now allow for their subscribers and users to access their device over the internet and remotely destroy all of the data contained on the device. For that reason, the device may only be powered in a secure environment or, if possible, started in "flight mode" which disables access to the network. Unlike typical computers, many mobile electronic devices do not have hard drives or hard drive equivalents and store information in volatile memory within the device or in memory cards inserted into the device. Current technology provides some solutions for acquiring some of the data stored in some mobile electronic device models using forensic hardware and software. Even if some of the stored information on the device may be acquired forensically, not all of the data subject to seizure may be so acquired. For devices that are not subject to forensic data acquisition or that have potentially relevant data stored that is not subject to such acquisition, the examiner must inspect the device manually and record the process and the results using digital photography. This process is time and labor intensive and may take weeks or longer.

35. Following the issuance of this warrant, I will collect the **Target Device** and subject it to analysis. All forensic analysis of the data contained within the **Target Device** and its memory card(s) will employ search protocols directed exclusively to the identification and extraction of data within the scope of this warrant.

36. Based on the foregoing, identifying and extracting data subject to seizure pursuant to this warrant may require a range of data analysis techniques, including manual review, and, consequently, may take weeks or months. The personnel conducting the identification and extraction of data will complete the analysis within ninety (90) days, absent further application to this court.

GENUINE RISK OF DESTRUCTION OF DATA

37. Based upon my experience and training, and the experience and training of other law enforcement agents with whom I have communicated, electronically stored data may be permanently deleted or modified by users possessing basic computer skills. In this case, no genuine risk of destruction exists as the property to be searched is already in the custody of law enforcement personnel.

PRIOR ATTEMPTS TO OBTAIN DATA

38. No prior attempts have been made by law enforcement to attempt to obtain data from the **Target Device**.

//

//

//

//

//

//

//

//

//

//

//

//

CONCLUSION

39. Based on the foregoing, I believe there is probable cause to believe items that constitute evidence, fruits, and instrumentalities of violations of federal criminal law, namely, 18 U.S.C. §§ 1349 and 1956(h) as described in Attachment B will be found in the properties to be searched, as provided in Attachment A.

Courtney M. McGuire

Courtney M. McGuire
Special Agent
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 30th day of March, 2023.

Barbara L. Major

HONORABLE **Barbara L. Major**
United States Magistrate Judge

ATTACHMENT A

ITEMS TO BE SEARCHED

The property/items to be searched is/are described as follows:

1. Apple iPhone, IMEI 356715110833004 **(Target Device)**

Target Device is currently being held at the San Diego Police Department, 1401 Broadway, San Diego, CA 92101.

ATTACHMENT B

ITEMS TO BE SEIZED

Authorization to search the cellular telephone described in Attachment A includes the search of disks, memory cards, deleted data, remnant data, slack space, and temporary or permanent files contained on or in the cellular telephones. The seizure and search of the cellular telephone will be conducted in accordance with the affidavit submitted in support of the warrant.

The evidence to be seized from the cellular telephones will be electronic records, communications, and data such as emails, text messages, photographs, audio files, video, telephone numbers, contact information, web browsing history, documents, data stored within applications, and location data, for the period of July 1, 2020 up to and including and August 31, 2022:

a. tending to identify travel to or presence at locations involved in wire fraud or money laundering;

b. tending to identify accounts, facilities, storage devices, and/or services—such as email addresses, IP addresses, and phone numbers—used to facilitate wire fraud and/or money laundering;

c. tending to identify co-conspirators, criminal associates, or others involved in wire fraud and/or money laundering;

d. tending to identify funding sources, bank accounts, and financing methods involved in wire fraud and/or money laundering;

e. tending to identify the user of, or persons with control over or access to, the subject phone; and/or

f. tending to place in context, identify the creator or recipient of, or establish the time of creation or receipt of communications, records, or data involved in the activities described above.

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

The seizure and search of the cellular phones shall follow the procedures outlined in the methodology section in the supporting affidavit. Deleted data, remnant data, slack space, and temporary and permanent files on the cellular phones may be searched for the evidence above.