UNITED STATES DISTRICT COURT

for the

Central 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)* A blue cellphone, model "BLU," with serial number 2110018018099565, as more fully described in Attachment A	)	Case No. 2:20-mj-04576

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. § 922(g)	Felon in Possession of a Firearm

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/ Brian De Jesus

Applicant's signature

Brian De Jesus, 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.

Date: _____

Judge's signature

City and state: Los Angeles, CA

Honorable Patricia Donahue

Printed name and title

ATTACHMENT A

PROPERTY TO BE SEARCHED

The following digital device, seized on November 3, 2019 by LASD and currently in the custody of the FBI in Lancaster, CA:

1. One BLU model cellphone, blue in color, with serial #2110018018099565, as depicted in the photograph below (the "SUBJECT DEVICE").

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of Title 18, United States Code, Sections 922(g) (Felon in Possession of a Firearm) (the "SUBJECT OFFENSE"), namely:

a. Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

b. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the above-named violation;

c. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violation;

d. Records, documents, programs, applications, materials, or conversations relating to the sale or purchase of guns or ammunition, including correspondence, receipts, records,

and documents noting prices or times when guns or ammunition were bought, sold, or otherwise distributed;

e. Audio recordings, pictures, video recordings, or still captured images related to the purchase, sale, transportation, or distribution of guns or ammunition;

f. Contents of any calendar, date book, phone notes, memos, or similar;

g. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations; and

h. The SUBJECT DEVICE which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense, and forensic copies thereof.

i. With respect to the SUBJECT DEVICE containing evidence falling within the scope of the foregoing categories of items to be seized:

i. 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;

ii. 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;

iii. evidence of the attachment of other devices;

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

v. evidence of the times the device was used;

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

vii. 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;

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

ix. 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.

2. 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.

II. SEARCH PROCEDURE FOR DIGITAL DEVICE(S)

3. In searching the SUBJECT DEVICE (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") may search the SUBJECT DEVICE capable of being used to facilitate the above-listed violations or containing data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search the SUBJECT DEVICE where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of the SUBJECT DEVICE as soon as is practicable but not to exceed 120 days from the date of issuance of the warrant. The government will not search the digital device(s) beyond this 120-day period without obtaining an extension of time order from the Court.

d. 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 the SUBJECT DEVICE capable of containing any of the items to be seized to the search protocols to determine whether the SUBJECT DEVICE and any data thereon falls within the scope of the 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 scope of the 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.

e. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

f. If the search determines that the SUBJECT 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 SUBJECT DEVICE and delete or destroy all forensic copies thereof.

g. If the search determines that the SUBJECT 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.

h. If the search determines that the SUBJECT 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.

i. The government may also retain a SUBJECT 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.

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

4. 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.

5. During the execution of this search warrant, law enforcement is permitted to (1) depress DARNELL ST. CLAIR's thumb- and/or fingers onto the fingerprint sensor of the SUBJECT DEVICE (only if 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 DARNELL ST. CLAIR's face with his or her 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.

6. 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 search of digital devices pursuant to any other court order.

AFFIDAVIT

I, Brian De Jesus, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of an application for a warrant to search a blue cellphone, model "BLU," with serial number 2110018018099565 (the "SUBJECT DEVICE"), in the custody of the Federal Bureau of Investigation, in Lancaster, California, as described more fully in Attachment A.

2. The requested search warrant seeks authorization to seize evidence, fruits, or instrumentalities of violations of Title 18, United States Code, Section 922(g) (Felon in Possession of a Firearm)(the "SUBJECT OFFENSE"), as described more fully in Attachment B. Attachments A and B are incorporated herein by reference.

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested search warrant, and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. BACKGROUND OF AFFIANT

4. I am a Special Agent with the Federal Bureau of Investigation and have been so employed since July 2018. I am currently assigned to the FBI Los Angeles Division's Lancaster Resident Agency. I attended the FBI Academy in Quantico, Virginia, which included training on money laundering offenses, investigations involving the sexual exploitation of children, and the distribution of narcotics. I have also had training on firearm offenses. Before joining the FBI, I worked for approximately four years as a New Jersey State Trooper.

III. SUMMARY OF PROBABLE CAUSE

5. At approximately 2:20 a.m. on November 3, 2019, a deputy with the Los Angeles Sheriff's Department ("LASD") observed a suspected drunk driver in a silver Toyota Camry ("Camry") committing several traffic violations. The driver failed to pull over after the deputy attempted a traffic stop, leading the deputy on a vehicle chase which ultimately ended when the Camry hit a curb.

6. After hitting the curb, the driver and passenger, who was later identified as DARNELL CORNELIUS ST. CLAIR, immediately fled the scene on foot. Moments later, LASD deputies found and detained ST. CLAIR while the driver escaped. While officers were detaining ST. CLAIR, they conducted a pat-down search and found a loaded handgun on him.

7. A subsequent records check determined ST. CLAIR was a convicted felon. Deputies later found the SUBJECT DEVICE in the Camry.

IV. STATEMENT OF PROBABLE CAUSE

8. Based on my review of law enforcement reports, conversations with other law enforcement agents, and my own knowledge of the investigation, I am aware of the following:

A. LASD Observes a Suspected Drunk Driver

9. At approximately 2:20 a.m. on November 3, 2019, LASD Deputy Jonathan Torsney observed the Camry committing multiple vehicle code violations, including tailgating and failing to stay within its lane. The deputy also noted that the Camry had a burnt-out tail light and expired registration tags. Based on his training and experience, and the Camry's erratic movement, Deputy Torsney believed the driver of the Camry was intoxicated.

10. As a result of these traffic violations, Deputy Torsney attempted a traffic stop. The Camry did not stop and instead led the deputy on a vehicle chase.

B. ST. CLAIR Flees from the Camry

11. The Camry eventually hit a curb and came to a stop. Deputy Torsney then observed the driver, an unidentified male, and passenger, who was later identified as ST. CLAIR, immediately flee the Camry on foot, in the opposite direction of police. Deputy Torsney alerted dispatch of the suspects' flight and broadcasted their descriptions over the radio.

C. Deputies Apprehend ST. CLAIR and Find a Gun on Him

12. Approximately a minute later, ST. CLAIR was detained by other LASD deputies, who were in the area after responding to the earlier vehicle pursuit call. The deputies conducted a pat-down search of ST. CLAIR after detaining him and found a loaded,

tan and black, Smith & Wesson, model M&P 40, .40 caliber semi-automatic pistol, bearing serial number HMJ4106. Deputies were unable to locate the driver of the vehicle.

13. A records check revealed that ST. CLAIR was a convicted felon, sustaining felony convictions for robbery, carrying a loaded firearm, prohibited possession of a firearm, and conspiracy to distribute cocaine base. ST. CLAIR was arrested for being a felon in possession of a firearm.

D. Deputies Search the Abandoned Camry and Find the SUBJECT DEVICE

14. Deputies then conducted an inventory search of the abandoned Camry before towing it. During the search of the car, deputies found the SUBJECT DEVICE on the driver's side floorboard. LASD seized the SUBJECT DEVICE as evidence. The SUBJECT DEVICE was later transferred to the custody of the FBI.

V. TRAINING AND EXPERIENCE ON FIREARMS OFFENSES

15. From my training, personal experience, and the collective experiences relayed to me by other law enforcement officers who conduct firearms investigations, I am aware of the following:

a. Persons who possess, purchase, or sell firearms generally maintain records of their firearm transactions as items of value and usually keep them in their residence, or in places that are readily accessible, and under their physical control, such as in their digital devices. It has been my experience that prohibited individuals who own firearms illegally will keep the contact information of the individual

who is supplying firearms to prohibited individuals or other individuals involved in criminal activities for future purchases or referrals. Such information is also kept on digital devices.

b. Persons who also possess firearms, especially prohibited arms, sometimes jointly possess or share firearms with each other.

c. Many people also keep mementos of their firearms, including digital photographs or recordings of themselves possessing or using firearms on their digital devices. These photographs and recordings are often shared via social media, text messages, and over text messaging applications.

d. Those who illegally possess firearms often sell their firearms and purchase firearms. Correspondence between persons buying and selling firearms often occurs over phone calls, e-mail, text message, and social media message to and from smartphones, laptops, or other digital devices. This includes sending photos of the firearm between the seller and the buyer, as well as negotiation of price. In my experience, individuals who engage in street sales of firearms frequently use phone calls, e-mail, and text messages to communicate with each other regarding firearms that they sell or offer for sale. In addition, it is common for individuals engaging in the unlawful sale of firearms to have photographs of firearms they or other individuals working with them possess on their cellular phones and other digital devices as they frequently send these photos to each other to boast of their firearms possession and/or to facilitate sales or transfers of firearms.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

16. As used herein, the term "digital device" includes the SUBJECT DEVICE.

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

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

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

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

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

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

18. 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.

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

19. 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. The person who is in possession of a device or has the device among his or her belongings is likely a user of the device. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress ST. CLAIR's thumb- and/or fingers on the device(s); and (2) hold the device(s) in front of ST. CLAIR's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

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

///

///

///

VII. CONCLUSION

21. For all of the reasons described above, there is probable cause to believe that the items listed in Attachment B, which constitute evidence, fruits, and instrumentalities of violations of SUBJECT OFFENSE will be found on the SUBJECT DEVICE, as described in Attachment A.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 24th day of September, 2020.

_____

THE HONORABLE PATRICIA DONAHUE
UNITED STATES MAGISTRATE JUDGE