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

UNITED STATES DISTRICT COURT

for the

Central District of California

LODGED
CLERK, U.S. DISTRICT COURT
11/10/2021
CENTRAL DISTRICT OF CALIFORNIA
BY: jb DEPUTY

United States of America

v.

EDGAR SAUL HERNANDEZ,
JONATHAN JESUS PEREZ-MARTINEZ,

Defendant(s)

Case No. 2:21-mj-05153-DUTY

FILED
CLERK, U.S. DISTRICT COURT
11/10/2021
CENTRAL DISTRICT OF CALIFORNIA
BY: KL DEPUTY

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief. On or about the date(s) of November 9, 2021, in the county of Los Angeles in the Central District of California, the defendant(s) violated:

Code Section	*Offense Description*
21 U.S.C. §§ 841(a)(1), (b)(1)(A)(vi)	Distribution and Possession With Intent to Distribute Fentanyl

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/ Andre. D. LaMon Jr.
Complainant's signature

Andre. D. LaMon Jr., HSI 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: November 10, 2021

Alicia G. Rosenberg
Judge's signature

City and state: Los Angeles, California

Hon. Alicia G. Rosenberg, U.S. Magistrate Judge
Printed name and title

AUSA: Rachel N. Agress (x0487)

ATTACHMENT A

PROPERTY TO BE SEARCHED

The following digital devices (the "SUBJECT DEVICES"), seized on November 9, 2021 and currently maintained in the custody of Homeland Security Investigations, in Los Angeles, California:

1. a blue iPhone 12 Pro Max in clear case with a "Billionaire Boys" Club sticker ("SUBJECT DEVICE 1");

2. a black Samsung with serial number 357014532269263 ("SUBJECT DEVICE 2");

3. a blue Motorola with no case ("SUBJECT DEVICE 3");

4. a black iPhone ("SUBJECT DEVICE 4"); and

5. a black Samsung with serial number 357014531754505 ("SUBJECT DEVICE 5").

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 21 U.S.C. § 841(a)(1) (possession with intent to distribute controlled substances) and 21 U.S.C. § 846 (conspiracy and attempt to distribute controlled substances) (the "Subject Offenses"), 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 violations;

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 violations;

d. Records, documents, programs, applications, materials, or conversations relating to the trafficking of drugs, including ledgers, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times when drugs 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 drugs;

f. Contents of any calendar or date book;

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

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

i. With respect to any 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 THE SUBJECT DEVICES

3. In searching the SUBJECT DEVICES (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any 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 each 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 DEVICES 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 each 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 [, including to search for known images of child pornography.]

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 a 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 a 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 DEVICES, 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 Edgar Saul HERNANDEZ's ("HERNANDEZ") and Jonathan Jesus PEREZ-MARTINEZ's ("PEREZ-

MARTINEZ") thumb- and/or fingers onto the fingerprint sensor of the SUBJECT DEVICES (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 HERNANDEZ's and PEREZ-MARTINEZ'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, Andre D. LaMon Jr, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint against Edgar Saul HERNANDEZ ("HERNANDEZ") and Jonathan Jesus PEREZ-MARTINEZ ("PEREZ-MARTINEZ"), for a violation of 21 U.S.C. § 841(a)(1): Possession with Intent to Distribute Fentanyl.

2. This affidavit is also made in support of an application for a warrant to search the following digital devices (collectively, the "SUBJECT DEVICES"), in the custody of Homeland Security Investigations, in Los Angeles, California, as described more fully in Attachment A:

a. a blue iPhone 12 Pro Max in clear case with a "Billionaire Boys" Club sticker ("SUBJECT DEVICE 1");

b. a black Samsung with IMEI 357014532269263 ("SUBJECT DEVICE 2");

c. a blue Motorola with no case ("SUBJECT DEVICE 3");

d. a black iPhone ("SUBJECT DEVICE 4"); and

e. a black Samsung with IMEI number 357014531754505 ("SUBJECT DEVICE 5").

3. The requested search warrant seeks authorization to seize evidence, fruits, or instrumentalities of violations of 21 U.S.C. § 841(a)(1) (possession with intent to distribute controlled substances) and 21 U.S.C. § 846 (conspiracy and

attempt to distribute controlled substances) (the "Subject Offenses"), as described more fully in Attachment B. Attachments A and B are incorporated herein by reference.

4. 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 complaint and search warrant and does not purport to set forth all 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

5. I am a Special Agent ("SA") with Homeland Security Investigations ("HSI") and have been so employed since September 2018. In May 2019, I completed the Criminal Investigator Training Program and Homeland Security Investigations Special Agent Training at the Federal Law Enforcement Training Center ("FLETC") and was assigned to Special Agent in Charge Los Angeles, California. I am currently assigned as a Special Agent with Los Angeles Interagency Metropolitan Police Apprehension Crime Taskforce ("LA IMPACT").

6. During my training at FLETC in Glynco, Georgia, I was trained in conducting criminal investigations and I received hundreds of hours of comprehensive, formalized instruction for investigations into such matters as the smuggling of narcotics

and other contraband; firearms trafficking and human trafficking; narcotics distribution and street gangs; money laundering; trade fraud; and asset identification, seizure and forfeiture. I have also participated in investigations concerning violations of immigration laws, narcotic possession/sales, and transnational street gangs. I am a graduate of California State University Long Beach, with a bachelor's degree in criminal justice.

7. In my experience in law enforcement, I have participated in numerous investigations involving smuggling and criminal street gangs, to include extortion, vehicle theft and vehicle smuggling, false document manufacturing and distribution, trafficking of firearms, and trade fraud. I have personally led numerous investigations involving the possession, manufacture, distribution, and importation of controlled substances from Mexico into the United States. I have also gained experience in interviewing, debriefing, surveilling, and arresting persons involved in narcotics violations and criminal gang activity.

III. SUMMARY OF PROBABLE CAUSE

8. In June 2021, via a telephone call, a confidential source (CS)[1] introduced an undercover agent ("UC-1") to a

[1] The CS has been providing information and assistance to local law enforcement and HSI investigators since June 2021. The CS has pre-2007 convictions for THC/cannabis distribution, resisting peace officers and disorderly conduct/false reports, property damage and theft, storage of weapons, battery, and driving offenses (including a DUI, reckless driving and driving with a suspended license). The CS has 2019 convictions for THC

(footnote cont'd on next page)

narcotics broker who is believed to reside in Mexico (the "broker"). UC-1 communicated with the broker via voice notes and messages on WhatsApp regarding potential narcotics sales.[2]

9. The broker arranged for a source of supply, later identified as PEREZ-MARTINEZ, to sell UC-1 five kilograms of fentanyl powder for $21,000 per kilogram. UC-1 and the broker also discussed the potential sale of 50 pounds of methamphetamine for $1,350 per pound. On November 9, 2021, UC-1 and a second undercover agent also posing as a drug dealer ("UC-2") drove to the meeting place to carry out the deal. PEREZ-MARTINEZ and a passenger, Individual A, arrived in a silver-grey Toyota, followed by HERNANDEZ in a silver Ford Focus. While HERNANDEZ and Individual A remained in the cars, PEREZ-MARTINEZ got out and showed the UCs a hard-sided plastic luggage case in the trunk of the silver Ford Focus. PEREZ-MARTINEZ indicated that the narcotics were in the luggage and UC-1 unzipped the luggage to reveal 4 bricks of suspected fentanyl.

10. HSI agents arrested PEREZ-MARTINEZ and HERNANDEZ. Agents recovered SUBJECT DEVICES 1 and 2 from PEREZ-MARTINEZ's person, SUBJECT DEVICE 3 from the center console of the silver

---

distribution. The CS provided information and assistance in connection with the investigation of the broker in this case, in exchange for consideration in an investigation into immigration violations by the CS. The CS has not been charged, has not currently entered into a deferred prosecution agreement with law enforcement, and has not received monetary compensation. The CS has provided information in this investigation that has proved to be true and correct and has not provided any information that was later determined to be false or otherwise unreliable.

[2] Unless otherwise stated, all calls referenced in this affidavit and all voice notes were recorded and were in Spanish. This affidavit relies on translations by a law enforcement native Spanish speaker.

Toyota that PEREZ-MARTINEZ was driving, and SUBJECT DEVICES 4 and 5 from the center console of the silver Ford Focus driven by HERNANDEZ. Agents also recovered a bag of approximately 8 ounces of a substance resembling crystal methamphetamine underneath HERNANDEZ's driver seat.

IV. STATEMENT OF PROBABLE CAUSE

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

A. Beginning in June 2021, UC-1 communicated with a Mexican narcotics broker about sales of narcotics

12. In June 2021, the CS introduced an undercover agent ("UC-1") to a narcotics broker who is believed to reside in Mexico (the "broker"). The introduction was made via telephone, and the CS introduced UC-1 to the broker as a drug dealer. Following the introduction, UC-1 and the broker began communicating via voice notes and messages on WhatsApp regarding potential narcotics sales.

13. On or about October 18, 2021, UC-1 and the broker began discussing a narcotics transaction for fentanyl and methamphetamine in Los Angeles, California. Via WhatsApp, the broker told UC-1 that the price for fentanyl per kilogram would be $24,000 and the price for methamphetamine per pound would be $1,150. The broker told UC-1 he would have a source of supply in California mail UC-1 a sample of the fentanyl to a shipping address provided by UC-1 to the broker.

14. On October 19, 2021, the broker sent UC-1 a photograph on WhatsApp of a UPS receipt. The receipt had tracking information for a package sent to UC-1's address by a source of supply in California. That day, HSI Los Angeles seized the package from the UPS Hub at the Ontario airport in Ontario, California. The package contained a small amount of white powdery substance, wrapped in green plastic, fabric softener dryer sheets and disinfectant wipes. On October 21, 2021, HSI Los Angeles and Customs and Border Protection Anti-Terrorism Contraband Enforcement Team personnel field tested the white powdery substance and it returned positive for fentanyl.

B. The broker arranges for PEREZ-MARTINEZ and HERNANDEZ to deliver 5 kilograms of fentanyl and 50 pounds of methamphetamine to UC-1

15. On or about November 5, 2021, UC-1 spoke with the broker via WhatsApp regarding the amount of fentanyl and methamphetamine being purchased in the upcoming narcotics transaction. UC-1 agreed to buy 5 kilograms of fentanyl and 50 pounds of methamphetamine from a then unknown source of supply in California for $172,500, on November 9, 2021.

16. On November 9, 2021, UC-1 spoke with the broker via WhatsApp and was informed that the narcotics would be arriving in two separate cars—a silver-gray car and a silver Ford Focus. UC-1 was also informed that the source of supply would first deliver four kilograms of fentanyl, and then would go back and retrieve the final kilogram of fentanyl. No final deal was reached at that time about the sale of 50 pounds of methamphetamine.

17. On November 9, 2021, law enforcement set up surveillance at the prearranged location where the drug sale was to take place, a shopping center parking lot in Los Angeles. Law enforcement identified a silver Toyota followed by a silver Ford Focus entering the parking lot. The two cars parked near UC-1's vehicle, and then the silver Ford Focus re-parked directly next to driver side of UC-1's vehicle. PEREZ-MARTINEZ got out of his car and directed HERNANDEZ to open the trunk of the silver Ford Focus. PEREZ-MARTINEZ showed the UCs a hard-sided plastic luggage case in the trunk of the silver Ford Focus. PEREZ-MARTINEZ indicated that the narcotics were in the luggage and UC-1 unzipped the luggage to reveal four bricks of a white powdery substance. PEREZ-MARTINEZ assisted UC-1 in moving the luggage case to the trunk of UC-1's vehicle.

C. Arrest of PEREZ-MARTINEZ and HERNANDEZ, and search of vehicles

18. HSI agents then detained and arrested PEREZ-MARTINEZ and HERNANDEZ.

19. Agents seized four bricks of what appeared to be pressed fentanyl, in red packaging and vacuum-packed bags, from inside the luggage case in the trunk of UC-1's vehicle. Based on my training and experience, the appearance of the packaging, and the communications leading up to the deal, I believe these bricks to contain fentanyl powder. Due to the dangerous nature of fentanyl and possible transdermal exposure, agents did not open the packages, but rather they are being sent to the Customs

and Border Protection ("CBP") laboratory in Long Beach, California, for testing and analysis.

20. Agents also seized a bag of approximately 8 ounces of a substance resembling crystal methamphetamine from underneath the driver's side of the silver Ford Focus, which is where HERNANDEZ was sitting. The suspected methamphetamine is also being sent to the the Customs and Border Protection ("CBP") laboratory for testing and analysis.

21. Agents recovered SUBJECT DEVICES 1 and 2 from PEREZ-MARTINEZ's pockets, SUBJECT DEVICE 3 from the center console of the silver Toyota which PEREZ MARTINEZ was driving, and SUBJECT DEVICES 4 and 5 from the center console of the silver Ford Focus, which HERNANDEZ was driving.

22. **PEREZ-MARTINEZ's and HERNANDEZ's Statements**

23. Both PEREZ-MARTINEZ and HERNANDEZ, after being advised of their Miranda rights and waiving their Miranda rights spoke with law enforcement. PEREZ-MARTINEZ admitted that he had arranged the logistics of transporting the narcotics to this location for sale. HERNANDEZ admitted assisting in transporting narcotics on occasions, including the methamphetamine found underneath his seat that day.

24. HERNANDEZ consented both orally and in writing to the search of SUBJECT DEVICES 4 and 5, and unlocked both phones for law enforcement, allowing law enforcement to access the contents of SUBJECT DEVICES 4 and 5. Law enforcement found messages relating to distribution-level amounts of narcotics, including fentanyl.

V. TRAINING AND EXPERIENCE ON DRUG OFFENSES

25. Based on my training and experience and familiarity with investigations into drug trafficking conducted by other law enforcement agents, I know the following:

a. Drug trafficking is a business that involves numerous co-conspirators, from lower-level dealers to higher-level suppliers, as well as associates to process, package, and deliver the drugs and launder the drug proceeds. Drug traffickers often travel by car, bus, train, or airplane, both domestically and to foreign countries, in connection with their illegal activities in order to meet with co-conspirators, conduct drug transactions, and transport drugs or drug proceeds.

b. Drug traffickers often maintain books, receipts, notes, ledgers, bank records, and other records relating to the manufacture, transportation, ordering, sale and distribution of illegal drugs. The aforementioned records are often maintained where the drug trafficker has ready access to them, such as on their cell phones and other digital devices.

c. Communications between people buying and selling drugs takes place by telephone calls and messages, such as e-mail, text messages, and social media messaging applications, sent to and from cell phones and other digital devices. This includes sending photos or videos of the drugs between the seller and the buyer, the negotiation of price, and discussion of whether or not participants will bring weapons to a deal. In addition, it is common for people engaged in drug trafficking to have photos and videos on their cell phones of drugs they or

others working with them possess, as they frequently send these photos to each other and others to boast about the drugs or facilitate drug sales.

d. Drug traffickers often keep the names, addresses, and telephone numbers of their drug trafficking associates on their digital devices. Drug traffickers often keep records of meetings with associates, customers, and suppliers on their digital devices, including in the form of calendar entries and location data.

e. Individuals engaged in the illegal purchase or sale of drugs and other contraband often use multiple digital devices.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

26. As used herein, the term "digital device" includes the SUBJECT DEVICES.

27. 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.

28. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it can take a substantial period of time to search a digital device for many 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.

c. Given the total number of digital devices (six) and the fact that the Mexican broker was known to communicate in Spanish via lengthly voice-notes sent on Whatsapp, which can only be analyzed for responsive content after being listened to in their entirety and translated, it may take substantial time to conduct a complete and accurate analysis of data on digital devices.

29. 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 HERNANDEZ's and PEREZ-MARTINEZ's thumb-

and/or fingers on the device(s); and (2) hold the device(s) in front of HERNANDEZ's and PEREZ-MARTINEZ's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

30. In addition to what has been described herein, the United States has attempted to obtain this data by requesting consent from HERNANDEZ and PEREZ-MARTINEZ to access the information on the SUBJECT DEVICES. HERNANDEZ consented both orally and in writing to the search of SUBJECT DEVICES 4 and 5, and unlocked both phones for law enforcement, allowing law enforcement to access the contents of SUBJECT DEVICES 4 and 5.

31. 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

32. For all of the reasons described above, there is probable cause to believe that HERNANDEZ and PEREZ-MARTINEZ have committed a violation of 21 U.S.C. § 841(a)(1): Possession with

Intent to Distribute Fentanyl. There is also probable cause that the items to be seized described in Attachment B will be found in a search of the SUBJECT DEVICES 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 9TH day of November 2021.

Alicia G. Rosenberg

THE HONORABLE ALICIA G. ROSENBERG
UNITED STATES MAGISTRATE JUDGE