

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, 1 Apple Park Way, Cupertino, California 95014  
(Accounts: 20298183955, 11893452869)

Case No. '24 MJ4262

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 Att.A

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

See Att. 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 USC Secs. 1203, 841, 848	Conspiracy to take hostages resulting in death, drug trafficking, intentional killing while engaged in drug trafficking

The application is based on these facts:

- 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.

  
Applicant's signature

Jesse Crim, 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: November 6, 2024

  
Judge's signature

City and state: San Diego, CA

Benjamin J. Cheeks  
Printed name and title



1 following paragraphs and in Attachments A and B, which are attached hereto  
2 incorporated herein.

### 3 **TRAINING & EXPERIENCE**

4 3. I am an investigative or law enforcement officer within the meaning of  
5 Title 18, United States Code, Section 2510(7); that is, an officer of the United States,  
6 who is empowered by law to conduct investigations of and to make arrests for  
7 offenses enumerated in Title 18, United States Code, Section 2516. I have been  
8 employed as a Special Agent with the Federal Bureau of Investigation (FBI) since  
9 September of 2014. Prior to my appointment to the FBI, I served as an Infantry  
10 Officer in the United States Army, First Armored Division. As an Infantry Officer  
11 I completed Ranger School and conducted a combat deployment to Iraq as a  
12 Battalion Scout Platoon Leader. I subsequently worked for three years as a  
13 supervisor at a subsea controls manufacturing group in Houston. My formal  
14 education consists of two undergraduate degrees from Louisiana State University. I  
15 am presently assigned to the FBI San Diego Strike Force (SDSF). The SDSF  
16 investigates crimes committed by drug trafficking organizations (DTOs) and I have  
17 been involved in numerous investigations involving individuals and criminal  
18 organizations involved in drug trafficking, money laundering, and crimes of violence  
19 associated with drug trafficking organizations. Prior to my assignment with the  
20 SDSF, I completed the 21-week FBI Academy and was trained in investigative  
21 techniques, procedures, and strategies.

22 4. I have also received specialized training in transnational organized  
23 crime and money laundering techniques utilized by the DTOs. I have also  
24 participated in numerous investigations in which members of drug trafficking  
25 organizations engaged in extortion, kidnapping, hostage taking, armed robbery, and  
26 murder relied heavily upon telephone communication to include the use of  
27 messaging applications such as WhatsApp, e-mail services, and cellular phones to

1 communicate with associates and co-conspirators. Through my investigations, my  
2 training and experience, and discussions with other law enforcement personnel, I  
3 have become familiar with the tactics and methods used by drug traffickers to  
4 smuggle and safeguard controlled substances, to distribute controlled substances, to  
5 collect and launder the proceeds from the sale of controlled substances, and commit  
6 violent crimes associated and inherent to drug trafficking such as kidnapping,  
7 extortion, armed robbery, and murder. My knowledge of the matters contained in  
8 this affidavit is based upon my personal knowledge, information provided to me by  
9 other law enforcement officers/agents, and witnesses.

10 5. The information set forth in this affidavit is based on my own personal  
11 knowledge, knowledge obtained from other individuals during my participation in  
12 this investigation, including other law enforcement officers, my review of  
13 documents and computer records related to this investigation, communications with  
14 others who have personal knowledge of the events and circumstances described  
15 herein, and information gained through my training and experience. Because this  
16 affidavit is submitted for the limited purpose of obtaining a search warrant for the  
17 **Subject Accounts**, it does not set forth each and every fact that I or others have  
18 learned during the course of this investigation, but only contains those facts believed  
19 to be necessary to establish probable cause.

## 20 **FACTS IN SUPPORT OF PROBABLE CAUSE**

### 21 **A. Background of the Case**

22 6. The FBI is investigating the kidnapping and murder of Miguel Anthony  
23 Rendon, a United States Citizen who was kidnapped from a hotel in Tijuana, Mexico  
24 on the night of Friday May 29, 2020. To date, this investigation has resulted in the  
25 indictment of five persons in connection with the kidnapping, hostage taking, and  
26 intentional killing of Rendon. These persons are Brian Alexis PATRON Lopez,  
27 Alan LOMELI Luna, Jonathan MONTELLANO Mora, Wyatt VALENCIA

1 Pacheco, and Luis DORANTES Rivera. LOMELI, VALENCIA, MONTELLANO,  
2 and DORANTES have all pled guilty to their roles in the crime. PATRON was  
3 extradited from Mexico to the United States on June 14, 2024, and is set for trial on  
4 January 13, 2025.

5 7. To date, investigators have reconstructed the events surrounding  
6 Rendon’s kidnapping, hostage taking, and murder. The facts presented herein were  
7 obtained from multiple Facebook search warrants --which revealed extensive  
8 communications between the participants of the crime before, during, and after the  
9 events— along with interviews of the victim’s family and cooperators. The  
10 cooperators provided their recollection of the events, which was corroborated  
11 extensively with other evidence and with one another’s testimony.

12 8. In short, the FBI’s investigation has shown that PATRON participated  
13 in the kidnapping, hostage taking, and murder of Rendon. PATRON and others  
14 kidnapped Rendon from the “El Parador” Motel on the night of May 29, 2020. The  
15 events were precipitated by Rendon stealing a quantity of methamphetamine from a  
16 narcotics trafficking cell that included PATRON. At the Parador, PATRON and  
17 others beat Rendon and then dragged him to a waiting vehicle. Over the next 17 to  
18 24 hours, Rendon was held hostage at several locations in Tijuana, Mexico. During  
19 this time, multiple witnesses observed PATRON beat Rendon, conduct ransom calls  
20 to Rendon’s family, and discuss plans to murder Rendon.

21 9. On or about the evening of May 30, 2020, PATRON murdered Rendon  
22 while LOMELI acted as a lookout. PATRON boasted about the killing to  
23 VALENCIA, MONTELLANO, and DORANTES, and several witnesses also  
24 watched a video recording of the murder that depicted PATRON shooting Rendon  
25 with a handgun. (The government does not yet possess this video.) The specific  
26 location, circumstances, number of gunshots, and manner of death were all  
27 separately corroborated by cooperators. One cooperator provided the location of the

1 murder. The FBI followed up with Mexican law enforcement, who identified a body  
2 at that location that matched Rendon’s description. An autopsy of the body  
3 identified Rendon and confirmed the cause of death (multiple gunshot wounds to the  
4 head), consistent with what the cooperators had previously told the FBI.

5 RENDON Steals Methamphetamine

6 10. Beginning on May 28, 2020, Rendon conspired with an associate to  
7 steal three pounds of crystal methamphetamine from LOMELI, the user of a  
8 Facebook account with the display name “AL LM.” Facebook communications and  
9 testimony from cooperators confirmed that Rendon was hired to receive and  
10 smuggle narcotics from Tijuana, Mexico to the United States. Rendon met in person  
11 with WYATT and LOMELI on the evening of May 28, 2020 to receive the narcotics  
12 he was hired to cross. Rendon then fled and stole the narcotics. After committing  
13 the theft, at 8:22 pm, Rendon sent an associate a photograph of the  
14 methamphetamine that he had stolen, and explained that it weighed three pounds.  
15 The photograph appeared to depict a white crystalline material in plastic packaging,  
16 consistent with the appearance of crystal methamphetamine.

17 11. One minute after Rendon sent the above-described photograph, at 8:23  
18 pm, WYATT, the user of the Facebook account “JC HF,” contacted Rendon via  
19 Facebook messenger. WYATT threatened Rendon and demanded that Rendon  
20 return the stolen narcotics. On May 29, 2020, at 12:42am, WYATT and PATRON  
21 discussed the situation, with WYATT explaining that he was talking to “Rendon.”  
22 WYATT relayed that Rendon claimed he had panicked and got busted after he  
23 crossed. Rendon claimed he was released and said that he would send a photo of the  
24 “document<sup>1</sup>” tomorrow. PATRON directed WYATT to tell Rendon that they

25 \_\_\_\_\_  
26 <sup>1</sup> For context, the “document” is a reference to a Notice to Appear and seizure notice,  
27 which law enforcement provided to prospective defendants during COVID, attesting  
to the seizure of the drugs and setting a date for the defendant to appear in Court.

1 needed to see him in person for the document, and that there was no problem if there  
2 was a document. WYATT said that Rendon was asking where he needed to meet  
3 PATRON (at which “plaza”), but PATRON did not respond in writing to this  
4 account.

#### 5 RENDON is Kidnapped

6 12. On May 29, 2020, Rendon traveled to Tijuana from San Diego to a  
7 motel called “Motel El Parador.”<sup>2</sup> MONTELLANO and an associate named  
8 Kenneth RIVERA learned from persons in contact with Rendon of Rendon’s plans  
9 to travel to the Parador.

10 13. Video surveillance footage from the Parador later obtained by the FBI  
11 showed Rendon being forcibly removed from a hotel parking lot by three males, one  
12 of whom was holding a handgun, on the night of May 29, 2020. Video surveillance  
13 footage shows that a late model BMW X5 model sport utility vehicle belonging to  
14 RIVERA was used by the males during the kidnapping event. Cooperators have  
15 identified PATRON as the male holding the handgun depicted in the video  
16 surveillance footage.

#### 17 The Hostage Takers Contact RENDON’s Family and Demand a Ransom

18 14. From the Parador, Rendon was taken hostage and subsequently moved  
19 to several locations around Tijuana, Mexico. In the early morning of May 30, 2020,  
20 Rendon’s mother began receiving ransom demands from two Mexican telephone  
21 numbers in the amount of \$2,000 to \$3,000 USD. Both phone numbers have been  
22 conclusively linked to LOMELI. The cooperators witnessed PATRON making  
23 these calls firsthand. The hostage takers allowed Rendon’s mother and stepfather to  
24 participate in a video chat with Rendon. Rendon’s parents observed that Rendon had  
25 been severely beaten and was bleeding from the nose and mouth. The hostage takers

---

26 <sup>2</sup> “Motel El Parador” is located at Blvd. Cuauhtémoc Sur Pte. 405, Madero Sur,  
27 22046 Tijuana, B.C., Mexico.

1 indicated the kidnapping occurred, because Rendon had stolen narcotics, specifically  
2 two to three pounds of crystal methamphetamine.

3 15. Evidence in the form of social media conversations and testimony from  
4 cooperators demonstrate that Rendon was held hostage for several hours on the night  
5 to morning of May 30, 2020 at the “Motel Luxor.” Conversations on the morning  
6 of May 30, 2020 between LOMELI and WYATT show that the pair discussed  
7 ongoing plans to murder Rendon. As these conversations developed, WYATT, who  
8 was not present at the hotel demanded that his brother Guillermo Adrian Valencia  
9 Pacheco (ADRIAN) be allowed to leave before they killed Rendon. A long  
10 conversation between WYATT and LOMELI developed as WYATT pled with  
11 LOMELI to arrange for an “Uber” to pick up ADRIAN and remove him from the  
12 situation at the Luxor. During this conversation, WYATT also asked PATRON to  
13 order an Uber for “Eydri” (ADRIAN). PATRON responded “I had already told –  
14 him.”

15 RENDON is murdered

16 16. The cooperators all state that Rendon was then transported to the “El  
17 Lago” neighborhood in Tijuana, Mexico, where PATRON executed Rendon by  
18 shooting him multiple times in the head with a handgun. The specific location,  
19 circumstances, number of gunshots, and manner of death are consistent across the  
20 cooperators’ accounts. Testimony from the witnesses enabled the FBI to coordinate  
21 with Mexican law enforcement to locate and identify Rendon’s remains.

22 17. On March 11, 2022 Rendon’s remains were transferred to the United  
23 States where an autopsy was conducted. The condition of the remains corroborated  
24 the cooperators’ testimony that Rendon was killed with multiple shots to the head  
25 with a small caliber handgun round.

26 18. The cooperators also stated that RENDON’s murder was videotaped.  
27 Some of the cooperators saw the videotape. One of them stated that PATRON kept



1 the video on his cellular phone and would share the video with others via “Airdrop”  
2 (a feature specific to Apple iPhones). Two of them described the video depicting  
3 PATRON executing Rendon by shooting multiple shots near Rendon’s ear with a  
4 handgun. Others did not personally see the video, but explained that PATRON  
5 boasted to them that the murder was captured on video.

6 19. Throughout the course of the investigation the FBI has obtained and  
7 reviewed search warrant results from Facebook Accounts for all of the subjects and  
8 the victim named above. A review of these Facebook accounts found extensive  
9 evidence that PATRON was directly involved in narcotics trafficking, specifically  
10 the deployment of persons to body carry narcotics from Mexico into the United  
11 States. Testimony from witnesses described that PATRON, LOMELI, WYATT,  
12 and MONTELLANO all cooperated with one another to traffic narcotics into the  
13 United States.

#### 14 **B. Evidence Specific to Subject Accounts 1 and 2**

15 20. Although the FBI has located one account for PATRON, I believe that  
16 PATRON, like others implicated in this offense, had multiple social media accounts.  
17 The FBI has also been told that PATRON kept a copy of the murder video. The FBI  
18 seeks to search additional accounts controlled by PATRON, such as **Subject**  
19 **Accounts 1 and 2**, to identify additional probative evidence, including the video of  
20 RENDON’s murder.

21 21. During the course of the investigation, the FBI has conclusively linked  
22 the phone number +52-664-819-5998 to PATRON. Specifically, the results of a  
23 search warrant for one of PATRON’s Google e-mail accounts,  
24 lmvpotosss@gmail.com, reflects a link to +52-664-819-5998. Second, an  
25 administrative subpoena to “Uber Technologies, INC” found that the same number  
26 was linked to PATRON’s Uber account.

1           22. On October 23, 2024, Apple Inc. provided a response to an  
2 administrative subpoena and identified +52-664-819-5998 as linked to two Apple  
3 accounts:

4           a. Account 20298183955, with the email e-mail address  
5           “patron\_101026@hotmail.com” (**Subject Account 1**)

6           b. Account 11893452869, with the e-mail address  
7           “16deadpools@gmail.com” (**Subject Account 2**);

8  
9           23. As to **Subject Account 1**, in addition to the link to PATRON’s phone  
10 number and name, the full name associated with the account is “Alexis Patron” at  
11 the address “Monte Himalaya” in Tijuana, Mexico. “Alexis Patron” is a match to a  
12 portion of PATRON’s full name of Brian Alexis PATRON Lopez. PATRON’s  
13 address in Mexico at the time of Rendon’s kidnapping and murder was a house  
14 located on “Monte Himalaya, Lomas Conjunto Residencial, 22116, Tijuana, Baja  
15 California, Mexico,” which is also a match to the street address registered to **Subject**  
16 **Account 1**.

17           24. As to **Subject Account 2**, in addition to the link to PATRON’s phone  
18 number, the name for the account is “Thalia Leonardo Diaz.” Throughout the  
19 investigation we have found that PATRON repeatedly used variations of the name  
20 “Leobardo” as an alias. For example, his Uber account and one of his Facebook  
21 profiles was in the name “Leobardo Garcia.” PATRON’s co-conspirators also used  
22 “Leonardo” as an alias for PATRON. Per a search warrant review of the phone  
23 belonging to ADRIAN, PATRON’s same phone number that is linked to **Subject**  
24 **Accounts 1 and 2** (+52-664-819-5998) was stored under the contact name  
25 “Leonardo Garcia.” The address provided for **Subject Account 2** is “Av. De los  
26 pollos” in Tijuana, Mexico. This is a short street measuring less than a block in  
27 length that is located approximately 2.2 miles from PATRON’s residence. Lastly,

1 the associated e-mail account for the iCloud account is “16deadpools@gmail.com.”  
2 The “16” is noteworthy because on the date that **Subject Account 2** was created,  
3 PATRON was 16 years of age. Based on the account being linked to PATRON's  
4 phone number, the registration name being consistent with PATRON's alias, the  
5 registration e-mail being consistent with PATRON's age, and the short distance of  
6 the registration address to PATRON's known address, I believe that **Subject**  
7 **Account 2** was likewise controlled by PATRON.

#### 8 **E. Justification for Data and Date Range Sought**

9 25. The FBI seeks to search the **Subject Accounts** for evidence of the  
10 **Target Offenses** between the dates of January 1, 2020 to present. The evidence  
11 outlined above demonstrates that PATRON was a participant in Rendon's  
12 kidnapping, hostage taking, and murder, which occurred on May 29, 2020. Of  
13 relevance to the captioned application, the FBI's understanding of the sequence of  
14 these events can be largely attributed to extensive and detailed social media text  
15 message conversations shared between the co-conspirators before and during the  
16 crime. When the investigation obtained and reviewed Facebook search warrant  
17 results for these subjects, the FBI found that they all relied heavily on text message  
18 communications as a primary means of communication within their network of  
19 associates. Therefore, I believe that a search of the **Subject Accounts** will yield  
20 communications between the subjects of the prosecution that are relevant to the  
21 crimes being investigated.

22 26. By way of Facebook Messenger conversations, witness statements, and  
23 arrest records, the FBI has found that PATRON was directly involved in narcotics  
24 trafficking, specifically the recruitment of juveniles and young adults to body carry  
25 narcotics from Mexico into the United States. Evidence identified from Facebook  
26 search warrant results show that PATRON directly participated in multiple narcotics  
27 trafficking events as early as August 2019. Therefore I believe a search of the

1 **Subject Accounts** will also yield communications or media relevant to confirm  
2 PATRON's engagement in narcotics trafficking.

3 27. Additionally, based on my training and experience, subjects engaged in  
4 narcotics trafficking, murder, hostage taking, and kidnapping conspiracies will often  
5 use cellular phones to communicate with co-conspirators and to coordinate the crime  
6 before, during, and after it takes place. Therefore, I believe this search warrant will  
7 produce additional evidence of PATRON's involvement in narcotics trafficking, as  
8 well as the kidnapping, hostage taking, and murder of Rendon, to include  
9 photographs, videos, electronic data, and communications amongst co-conspirators.  
10 Further, in my training and experience, those engaged in these crimes may be  
11 involved in the planning and coordination of the criminal event in the days, weeks,  
12 and months prior to and after the actual event.

13 28. As the FBI has started arresting participants in the conspiracy in early  
14 June 2021 and through November 2023, ending with the arrest of PATRON in  
15 Mexico, it is very likely that this enforcement action spurred communications  
16 between PATRON and other co-conspirators and associates. Further, while  
17 PATRON has been in custody since his arrest on November 9, 2023, I seek data to  
18 the present date in order to determine if PATRON has employed any associates to  
19 attempt to delete the **Subject Accounts** or the data contained herein.

20 *Applicability of the **Subject Accounts***

21 29. Based upon my experience investigating violent crimes and the  
22 investigation in this case, I believe that the **Subject Accounts** may contain relevant  
23 evidence in this case. In addition, I know that recent calls made and received,  
24 telephone numbers, contact names, electronic mail (e-mail) addresses, appointment  
25 dates, text messages, pictures and other digital information may be uploaded and  
26 stored on the **Subject Accounts** and may identify the persons involved in the  
27 conspiracy. Accordingly, based upon my experience and training, consultation with

1 other law enforcement officers experienced in violent crime and narcotics trafficking  
2 investigations, and all the facts and opinions set forth in this affidavit, I believe that  
3 information relevant to PATRON’s activities, such as telephone numbers, made and  
4 received calls, contact names, electronic mail (e-mail) addresses, appointment dates,  
5 messages, pictures and other digital information are stored in the **Subject Accounts**.

6 30. Based on my training and experience, iCloud accounts, which contain  
7 saved data such as messages, videos, photographs, and other data, are relevant and  
8 material to the investigation of individuals who participate in violent crimes and  
9 narcotics trafficking because such information can help identify the subjects and  
10 their communications relating to the crime. Therefore, data sought under this  
11 warrant is relevant up to the date of this warrant for the **Subject Accounts**.

### 12 **INFORMATION REGARDING APPLE ID AND iCloud<sup>3</sup>**

13 31. Apple is a United States company that produces the iPhone, iPad, and  
14 iPod Touch, all of which use the iOS operating system, and desktop and laptop com-  
15 puters based on the Mac OS operating system.

16 32. Apple provides a variety of services that can be accessed from Apple  
17 devices or, in some cases, other devices via web browsers or mobile and desktop  
18 applications (“apps”). As described in further detail below, the services include  
19 email, instant messaging, and file storage:

---

21  
22 <sup>3</sup> The information in this section is based on information published by Apple  
23 on its website, including, but not limited to, the following document and webpages:  
24 “U.S. Law Enforcement Legal Process Guidelines,” available at  
<http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; “Create and  
25 start using an Apple ID,” available at <https://support.apple.com/en-us/HT203993>;  
26 “iCloud,” available at <http://www.apple.com/icloud/>; “iCloud: iCloud storage and  
27 backup overview,” available at <https://support.apple.com/kb/PH12519>; and “iOS  
Security,” available at  
[http://images.apple.com/privacy/docs/iOS\\_Security\\_Guide.pdf](http://images.apple.com/privacy/docs/iOS_Security_Guide.pdf).

1 a. Apple provides email service to its users through email addresses  
2 at the domain names mac.com, me.com, and icloud.com.

3 b. iMessage and FaceTime allow users of Apple devices to  
4 communicate in real-time. iMessage enables users of Apple devices to exchange  
5 instant messages (“iMessages”) containing text, photos, videos, locations, and  
6 contacts, while FaceTime enables those users to conduct video calls.

7 c. iCloud is a file hosting, storage, and sharing service provided by  
8 Apple. iCloud can be utilized through numerous iCloud-connected services, and can  
9 also be used to store iOS device backups and data associated with third-party apps.

10 d. iCloud-connected services allow users to create, store, access,  
11 share, and synchronize data on Apple devices or via icloud.com on any Internet-  
12 connected device. For example, iCloud Mail enables a user to access Apple-  
13 provided email accounts on multiple Apple devices and on icloud.com. iCloud  
14 Photo Library and My Photo Stream can be used to store and manage images and  
15 videos taken from Apple devices, and iCloud Photo Sharing allows the user to share  
16 those images and videos with other Apple subscribers. iCloud Drive can be used to  
17 store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud  
18 to be used to synchronize webpages opened in the Safari web browsers on all of the  
19 user’s Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers,  
20 and Keynote), enables iCloud to be used to create, store, and share documents,  
21 spreadsheets, and presentations. iCloud Keychain enables a user to keep website  
22 username and passwords, credit card information, and Wi-Fi network information  
23 synchronized across multiple Apple devices.

24 e. Game Center, Apple’s social gaming network, allows users of  
25 Apple devices to play and share games with each other.

1 f. Find My iPhone allows owners of Apple devices to remotely  
2 identify and track the location of, display a message on, and wipe the contents of  
3 those devices.

4 g. Location Services allows apps and websites to use information  
5 from cellular, Wi-Fi, Global Positioning System (“GPS”) networks, and Bluetooth,  
6 to determine a user’s approximate location.

7 h. App Store and iTunes Store are used to purchase and download  
8 digital content. iOS apps can be purchased and downloaded through App Store on  
9 iOS devices, or through iTunes Store on desktop and laptop computers running  
10 either Microsoft Windows or Mac OS. Additional digital content, including music,  
11 movies, and television shows, can be purchased through iTunes Store on iOS devices  
12 and on desktop and laptop computers running either Microsoft Windows or Mac OS.

13 33. Apple services are accessed through the use of an “Apple ID,” an ac-  
14 count created during the setup of an Apple device or through the iTunes or iCloud  
15 services. A single Apple ID can be linked to multiple Apple services and devices,  
16 serving as a central authentication and syncing mechanism.

17 34. An Apple ID takes the form of the full email address submitted by the  
18 user to create the account; it can later be changed. Users can submit an Apple-  
19 provided email address (often ending in @icloud.com, @me.com, or @mac.com) or  
20 an email address associated with a third-party email provider (such as Gmail, Yahoo,  
21 or Hotmail). The Apple ID can be used to access most Apple services (including  
22 iCloud, iMessage, and FaceTime) only after the user accesses and responds to a  
23 “verification email” sent by Apple to that “primary” email address. Additional email  
24 addresses (“alternate,” “rescue,” and “notification” email addresses) can also be  
25 associated with an Apple ID by the user.

26 35. Apple captures information associated with the creation and use of an  
27 Apple ID. During the creation of an Apple ID, the user must provide basic personal

1 information including the user's full name, physical address, and telephone numbers.  
2 The user may also provide means of payment for products offered by Apple. The  
3 subscriber information and password associated with an Apple ID can be changed  
4 by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In  
5 addition, Apple captures the date on which the account was created, the length of  
6 service, records of log-in times and durations, the types of service utilized, the status  
7 of the account (including whether the account is inactive or closed), the methods  
8 used to connect to and utilize the account, the Internet Protocol address ("IP  
9 address") used to register and access the account, and other log files that reflect usage  
10 of the account.

11 36. Additional information is captured by Apple in connection with the use  
12 of an Apple ID to access certain services. For example, Apple maintains connection  
13 logs with IP addresses that reflect a user's sign-on activity for Apple services such  
14 as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and  
15 iForgot pages on Apple's website. Apple also maintains records reflecting a user's  
16 app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime  
17 calls, and "mail logs" for activity over an Apple-provided email account. Records  
18 relating to the use of the Find My iPhone service, including connection logs and  
19 requests to remotely lock or erase a device, are also maintained by Apple.

20 37. Apple also maintains information about the devices associated with an  
21 Apple ID. When a user activates or upgrades an iOS device, Apple captures and  
22 retains the user's IP address and identifiers such as the Integrated Circuit Card ID  
23 number ("ICCID"), which is the serial number of the device's SIM card. Similarly,  
24 the telephone number of a user's iPhone is linked to an Apple ID when the user signs  
25 in to FaceTime or iMessage. Apple also may maintain records of other device  
26 identifiers, including the Media Access Control address ("MAC address"), the  
27 unique device identifier ("UDID"), and the serial number. In addition, information



1 about a user's computer is captured when iTunes is used on that computer to play  
2 content associated with an Apple ID, and information about a user's web browser  
3 may be captured when used to access services through icloud.com and apple.com.  
4 Apple also retains records related to communications between users and Apple  
5 customer service, including communications regarding a particular Apple device or  
6 service, and the repair history for a device.

7 38. Apple provides users with five gigabytes of free electronic space on  
8 iCloud, and users can purchase additional storage space. That storage space, located  
9 on servers controlled by Apple, may contain data associated with the use of iCloud-  
10 connected services, including: email (iCloud Mail); images and videos (iCloud  
11 Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spread-  
12 sheets, presentations, and other files (iWorks and iCloud Drive); and web browser  
13 settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud  
14 can also be used to store iOS device backups, which can contain a user's photos and  
15 videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Ser-  
16 vice ("MMS") messages, voicemail messages, call history, contacts, calendar events,  
17 reminders, notes, app data and settings, and other data. Records and data associated  
18 with third-party apps may also be stored on iCloud; for example, the iOS app for  
19 WhatsApp, an instant messaging service, can be configured to regularly back up a  
20 user's instant messages on iCloud.

21 39. Based upon my experience and training, consultation with other law  
22 enforcement officers experienced in violent crime and narcotics trafficking  
23 investigations, and all the facts and opinions set forth in this affidavit, I know that  
24 individuals involved in these crimes often utilize cell phones, including their  
25 associated iCloud accounts, in the weeks and months prior to, during, and after a  
26 violent crime or narcotics trafficking event, or after the arrest of a co-conspirator, so  
27 the **Subject Accounts** could contain:

- 1 a. Communications, photographs, videos, or other data depicting
- 2 narcotics, plans or attempts to smuggle and traffic narcotics, narcotics
- 3 proceeds,
- 4 b. Communications, photographs, videos, or other data depicting victims
- 5 and targets of violent crimes, the planning or commission of violent
- 6 crimes, and efforts to threaten victims or witnesses, collect ransoms,
- 7 and elude law enforcement,
- 8 c. Internet and web-search history relating to narcotics trafficking and
- 9 violent crimes;
- 10 d. Communications, photographs, videos, or other data shared with
- 11 coconspirators to coordinate and then execute narcotics trafficking
- 12 events and violent crimes, to include;
- 13 e. Celebratory remarks after the successful completion of a violent crime
- 14 or narcotics trafficking event;
- 15 f. Geo-locational information related to a violent crime such as where it
- 16 occurred and the location or remains of a victim during and after the
- 17 commission of the crime;

18 40. In my training and experience, evidence of who was using an Apple ID  
19 and from where, and evidence related to criminal activity of the kind described  
20 above, may be found in the files and records of the **Subject Accounts**. Likewise,  
21 this cellphone evidence, including iMessages and other communications backed up  
22 to **Subject Accounts**, may be used to establish the “who, what, why, when, where,  
23 and how” of the investigation into the kidnapping, hostage taking, and murder  
24 conspiracy as well as the associated narcotics trafficking activities of the target  
25 subjects, thus enabling the United States to establish and prove each element or,  
26 alternatively, to exclude the innocent from further suspicion.

27 41. For example in this case, the stored iMessages and contacts connected

1 to the **Subject Accounts** may provide direct communications between co-  
2 conspirators. It also be used to help identify known co-conspirators of whom are yet  
3 unidentified.

4 42. Activity over the **Subject Accounts** may also provide relevant insight  
5 into the account owner's state of mind as it relates to the offenses under  
6 investigation. For example, information on the account may indicate the owner's  
7 motive and intent to commit a crime (e.g., information indicating a plan to commit  
8 a crime), or consciousness of guilt (e.g., deleting account information in an effort to  
9 conceal evidence from law enforcement).

10 43. Other information connected to an Apple ID may lead to the discovery  
11 of additional evidence. For example, the identification of apps downloaded from  
12 App Store and iTunes Store may reveal services used in furtherance of the crimes  
13 under investigation or services used to communicate with co-conspirators. In  
14 addition, emails, instant messages, Internet activity, documents, and contact and  
15 calendar information can lead to the identification of co-conspirators and  
16 instrumentalities of the crimes under investigation.

17 44. Therefore, Apple's servers are likely to contain stored electronic  
18 communications and information concerning subscribers and their use of Apple's  
19 services. In my training and experience, such information may constitute evidence  
20 of violent crimes and narcotics trafficking conspiracies, including information that  
21 can be used to identify the account's user.

22 45. Based on the information provided above, I respectfully request  
23 permission to search the **Subject Accounts** for items listed in Attachment B  
24 beginning on January 1, 2020, up to and including the date of this warrant.

25 **INFORMATION TO BE SEARCHED AND ITEMS TO BE SEIZED**

26 46. I anticipate executing this warrant under the Electronic  
27 Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A)

1 and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the  
2 government copies of the records and other information (including the content of  
3 communications and stored data) particularly described in Section I of Attachment  
4 B. Upon receipt of the information described in Section I of Attachment B, FBI  
5 agents, or other federal agents, will review that information to locate the items  
6 described in Section II of Attachment B. The FBI issued a preservation letter for  
7 both accounts last week.

8 **CONCLUSION**

9 47. Based on all of the facts and circumstances described above, there is  
10 probable cause to conclude that the **Subject Accounts** contain evidence of violations  
11 of 18 U.S.C. §§ 1203 (Conspiracy to take Hostages Resulting in Death), 21 U.S.C.  
12 §§ 848(e)(1)(A) (Intentional Killing While Engaged in Drug Trafficking), and Title  
13 21 U.S.C. §§ 841 (Narcotics Trafficking).

14 48. There is probable cause to believe that evidence of illegal activities  
15 committed by PATRON continues to exist on the **Subject Accounts**. As stated  
16 above, I submit that the date range for this search to be from January 1, 2020, up to  
17 and including the date of this warrant.

18 //

19 //

20 //

21 //

22 //

23 //

24 //

25 //

26 //

27 //



**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with Apple IDs (“Subject Account”) affiliated with the below identifiers, that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Apple Park Way, Cupertino, CA 95014.

1. Apple Account Number 20298183955, registered to e-mail address “patron\_101026@hotmail.com” and
2. Apple account number 11893452869, registered to e-mail address “16deadpools@gmail.com”

**ATTACHMENT B**

**I. Service of Warrant**

The officer executing the warrant shall permit Apple Inc., as the custodian of the computer files described in Section II below, to locate the files and copy them onto removable electronic storage media and deliver the same to the officer.

**II. Items Subject to Seizure**

The following items are subject to seizure from the iCloud **Subject Accounts** (**Subject Account 1:** Apple Account Number 20298183955, registered to e-mail address “patron\_101026@hotmail.com” and **Subject Account 2:** Apple account number 11893452869, registered to e-mail address “16deadpools@gmail.com”) from January 1, 2020 up to and including the date of service of the warrant. To the extent that the information described in the Attachment A section is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government for each account or identifier listed in the Attachment A section:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account

1 status, associated devices, methods of connecting, and means and source of payment  
2 (including any credit or bank account numbers);

3 b. All records or other information regarding the devices associated with,  
4 or used in connection with, the account (including all current and past trusted or  
5 authorized iOS devices and computers, and any devices used to access Apple  
6 services), including serial numbers, Unique Device Identifiers (“UDID”),  
7 Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media  
8 Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”),  
9 Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers  
10 (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers  
11 (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated  
12 Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber  
13 Identities (“IMSI”), and International Mobile Station Equipment Identities  
14 (“IMEI”);

15 c. The contents of all emails associated with the account, including stored  
16 or preserved copies of emails sent to and from the account (including all draft emails  
17 and deleted emails), the source and destination addresses associated with each email,  
18 the date and time at which each email was sent, the size and length of each email,  
19 and the true and accurate header information including the actual IP addresses of the  
20 sender and the recipient of the emails, and all attachments;

21 d. The contents of all instant messages associated with the account,  
22 including stored or preserved copies of instant messages (including iMessages, SMS  
23 messages, and MMS messages) sent to and from the account (including all draft and  
24 deleted messages), the source and destination account or phone number associated  
25 with each instant message, the date and time at which each instant message was sent,  
26 the size and length of each instant message, the actual IP addresses of the sender and  
27



1 the recipient of each instant message, and the media, if any, attached to each instant  
2 message;

3 e. The contents of all files and other records stored on iCloud, including  
4 all iOS device backups, all Apple and third-party app data, all files and other records  
5 related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo  
6 Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes),  
7 iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact  
8 and buddy lists, notes, reminders, calendar entries, images, videos, voicemails,  
9 device settings, and bookmarks;

10 f. All activity, connection, and transactional logs for the account (with  
11 associated IP addresses including source port numbers), including FaceTime call  
12 invitation logs, messaging and query logs (including iMessage, SMS, and MMS  
13 messages), mail logs, iCloud logs, iTunes Store and App Store logs (including  
14 purchases, downloads, and updates of Apple and third-party apps), My Apple ID and  
15 iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone  
16 and Find My Friends logs, logs associated with web-based access of Apple services  
17 (including all associated identifiers), and logs associated with iOS device purchase,  
18 activation, and upgrades;

19 g. All records and information regarding locations where the account or  
20 devices associated with the account were accessed, including all data stored in  
21 connection with Location Services, Find My iPhone, Find My Friends, and Apple  
22 Maps;

23 h. All records pertaining to the types of service used;

24 i. All records pertaining to communications between Apple and any  
25 person regarding the account, including contacts with support services and records  
26 of actions taken;

27

1 j. All files, keys, or other information necessary to decrypt any data  
2 produced in an encrypted form, when available to Apple (including, but not limited  
3 to, the keybag.txt and fileinfolist.txt files;

4 k. Any other accounts linked to the subject accounts by cookie values,  
5 SMS, Recovery, Android device, Apple device, account mobile device, secondary  
6 email, or phone number;

7 h. Any records pertaining to the means and source of payment for services  
8 (including any credit card or bank account number or digital money transfer account  
9 information).

10 **III. Search of the Data**

11 The search of the data supplied by Apple pursuant to this warrant will be  
12 conducted by the Federal Bureau of Investigation as provided in the “Procedures For  
13 Electronically-Stored Information” section of the affidavit submitted in support of  
14 this search warrant and will be limited to the period of January 1, 2020, up to and  
15 including the date the warrant is served to Apple, and be further limited to:

16 a. Communications, records, images and attachments tending to discuss  
17 or suggest the operation, management and/or financing of illegal marijuana  
18 dispensaries;

19 b. Communications, records, images, and attachments tending to discuss  
20 or suggest the operation, management and/or financing of illegal marijuana  
21 dispensaries involving personal identification information and/or a “means of  
22 identification” (which includes names, social security numbers, credit histories,  
23 driver’s license information, addresses, e-mail addresses, account numbers, bank  
24 accounts, brokerage accounts, usernames, and passwords);

25 c. Communications, records, images, and attachments tending to discuss  
26 or suggest the operation, management and/or financing of illegal marijuana  
27 dispensaries involving wire transfers, withdrawals of monetary instruments, credit

1 card charges, debit card payments, court settlement disbursement, or bank account  
2 user information;

3 d. Communications, records, images, and attachments tending to identify  
4 the user(s) of the subject accounts, and any co-conspirators involved in the activities  
5 in III(a)-(c) above;

6 e. Communications, records, images, and attachments that provide  
7 context to any communications or records described above, such as messages sent  
8 or received in temporal proximity to any relevant electronic communications and  
9 any electronic communications tending to identify users of the subject accounts; and

10 f. Any other accounts linked to the subject account by cookie values,  
11 SMS, Recovery, Android device, Apple device, other mobile device, secondary  
12 email, or phone number;

13 which are evidence of violations of 18 U.S.C. §§ 1203 (Conspiracy to take Hostages  
14 Resulting in Death), 21 U.S.C. § 848(e)(1)(A) (Intentional Killing While Engaged  
15 in Drug Trafficking), and Title 21 U.S.C. §§ 841 (Narcotics Trafficking).  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27