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 iCloud, 1 Apple Park Way, Cupertino, CA 95014
re. the iCloud account affiliated with
Leon101026@hotmail.com

Case No. 24MJ4410

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A, incorporated herein by reference.

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

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. s. 841, 848(e)(1)(A), 18 U.S.C. s. 1203	Murder While Engaged In Drug Trafficking; Narcotics Trafficking ; Conspiracy to Commit Hostage Taking

The application is based on these facts:

See Attached Affidavit of FBI Special Agent Jenna Paisley

- ☑ 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.

Jenna Paisley
Applicant's signature

Jenna Paisley, 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: 11/22/2024

Allison H. Goddard
Judge's signature

City and state: San Diego, California

Hon. Allison H. Goddard United States Magistrate Judge
Printed name and title

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 associated with e-mail address "Leon101026@hotmail.com" and believed to be used by Brian Alexis PATRON Lopez

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 Account** (Apple Account registered to e-mail address Leon101026@hotmail.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 status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

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

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

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

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

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

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

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

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

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

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

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

III. Search of the Data

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

a. Communications, photographs, videos, or other data depicting narcotics, plans or attempts to smuggle and traffic narcotics, or narcotics proceeds,

b. Communications, photographs, videos, or other data depicting victims and targets of violent crimes, the planning or commission of violent crimes, and efforts to threaten victims or witnesses, collect ransoms, and elude law enforcement,

c. Internet and web-search history relating to narcotics trafficking and violent crimes;

d. Communications, photographs, videos, or other data shared with coconspirators to coordinate and then execute narcotics trafficking events and violent crimes;

e. Communications, photographs, videos, or other data amongst coconspirators to discuss narcotics trafficking or violent crimes after the commission of the crimes, including but not limited to efforts to evade law enforcement detection;

f. Geo-locational information related to a violent crime such as where it occurred and the location or remains of a victim during and after the commission of the crime;

g. Communications, records, images, and attachments tending to identify the user(s) of the subject accounts, and any co-conspirators involved in narcotics trafficking or violent crime activities;

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

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

which are evidence of violations of 18 U.S.C. § 1203 (Conspiracy to take Hostages Resulting in Death), 21 U.S.C. § 848(e)(1)(A) (Intentional Killing While Engaged in Drug Trafficking), and Title 21 U.S.C. § 841 (Narcotics Trafficking).

AFFIDAVIT IN SUPPORT OF

APPLICATIONS FOR SEARCH WARRANTS

I, Jenna Paisley, being duly sworn, state as follows:

INTRODUCTION

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with the following iCloud account:

a. iCloud Account associated with e-mail address "Leon101026@hotmail.com" and believed to be used by Brian Alexis PATRON Lopez (**Subject Account**)

between the dates of January 1, 2020 to present, for items which constitute evidence, fruits, and instrumentalities for violations of 18 U.S.C. § 1203 (Conspiracy to take Hostages Resulting in Death), 21 U.S.C. § 848(e)(1)(A) (Intentional Killing While Engaged in Drug Trafficking), and Title 21 U.S.C. § 841 (Narcotics Trafficking), (collectively, the Target Offenses) as more fully described in Attachment B. As provided attached, investigators have previously conducted a search of two Target Accounts belonging to Brian Alexis PATRON Lopez pursuant to a federal search warrant authorized by Magistrate Judge Benjamin J. Cheeks on November 6, 2024. The warrant authorized the release of material from the Target Accounts within the date range of January 1, 2020 and November 7, 2024. Investigators have since received a initially reviewed the returns for this warrant, and identified that PATRON controlled the target accounts. However, the search warrant results provided by Apple revealed that PATRON has another iCloud account previously unknown to investigators. Therefore, as supported by evidence below, I hereby request that a follow-on

search warrant be granted for **Subject Account**. The original search warrant for the Target Accounts is attached as Exhibit 1, and is incorporated to this affidavit in full.

2. For the reasons set forth below, I believe there is probable cause for the requested warrant for the **Subject Account**, the contents of which are stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Apple Park Way, Cupertino, California 95014. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B, which are attached hereto incorporated herein.

TRAINING & EXPERIENCE

3. I am a "law enforcement officer of the United States" within the meaning of Title 18, United States Code, Section 2510(7), who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 2516. I also am a Federal Law Enforcement Officer within the meaning of Rule 41(b) of the Federal Rules of Criminal Procedure, that is, a government agent engaged in the enforcement of the criminal laws of the United States, and thereby authorized to request issuance of federal search and seizure warrants. I am empowered to conduct investigations of, and to make arrests for, federal offenses

4. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed since February 2023. I am presently assigned to the San Diego Organized Crime Drug Enforcement Task Force (OCDETF) Strike Force. The OCDETF Strike Force primarily investigates Transnational Criminal Organizations (TCOs) originating in Mexico, Central, and South America. These investigations typically target the criminal activities of drug trafficking organizations (DTOs) and money laundering organizations (MLOs). I have been one of the lead agents on numerous OCDETF investigations. I have interviewed

numerous defendants, victims, witnesses, and informants who have direct knowledge of international contraband smuggling, money laundering, and violent criminal activity.

5. Prior to this assignment, I spent approximately five years as a Consular Officer for the United States Department of State. As a Consular Officer, I served at U.S. Consulate General Rio de Janeiro, U.S. Consulate General Sao Paulo, U.S. Consulate General Guayaquil, U.S. Embassy Santo Domingo and U.S. Embassy Kingston. I interviewed thousands of immigrant and non-immigrant visa applicants and led complex fraud investigations. I subsequently worked for two years as an immigration paralegal and consultant. I prepared sophisticated immigration and investor visa application packets in accordance with the Immigration and Nationality Act. My formal education consists of an undergraduate degree from University of Colorado at Boulder and a certificate in translation from University of Chicago. Through these positions, as well as my time spent at the 20-week FBI academy, I have been educated in investigative manners and have received specialized training in transnational organized crime, narcotics trafficking, and money laundering techniques commonly used by DTOs and MLOs. Through my investigations, my training and experience, and discussions with other law enforcement personnel, I have become familiar with the tactics and methods used by drug traffickers to smuggle and safeguard controlled substances, to distribute controlled substances, to collect and launder the proceeds from the sale of controlled substances, and commit violent crimes associated and inherent to drug trafficking such as kidnapping, extortion, armed robbery, and murder. These methods include the utilization of cellular telephones, e-mail services, social media platforms, applications with end-to-end encryption, false or fictitious identities, and compartmentalized and coded conversations to carry out criminal activity

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

FACTS IN SUPPORT OF PROBABLE CAUSE

A. Background of the Case

7. Please see Exhibit 1, the original search warrant, which I incorporate in full. The background of the case is specifically found in the affidavit of Exhibit 1, paragraphs 6–19.

B. Evidence Specific to Subject Account

8. Although the FBI has located two accounts for PATRON, I believe that PATRON had multiple social media and iCloud accounts. The FBI has also been told that PATRON kept a copy of the murder video. The FBI seeks to search additional accounts controlled by PATRON, such as the **Subject Account**, to identify additional probative evidence, including the video of RENDON's murder.

9. While reviewing the data provided by Apple in response to the original search warrant, the FBI found that one of the searched accounts, Account 20298183955 with associated e-mail address of patron_101026@hotmail.com, was controlled by PATRON and contained pertinent information. Specifically, a total of 206 photo records were produced in the search warrant production which range from approximately August of 2021 to April of 2022. The photographs consisted

primarily of self-taken photographs of PATRON. In addition, a screenshot of PATRON's Mexican identification information was found. The screenshot clearly depicts his full name and date of birth.

10. As to the **Subject Account**, within Account 20298183955, a "Note" created on 4/10/2022 was found which contained the following username/login information:

"Leon101026@hotmail.com

patronlopez2323

Pw cloud: PatronLopez2323"

11. In addition to being found within an Apple account controlled by PATRON, the number sequence "101026" is present in both the associated email from the original search warrant (patron_101026@hotmail.com) and the **Subject Account.** As to the "Leon" portion of the **Subject Account** email address, the FBI has found throughout the investigation that PATRON repeatedly used variations of the name "Leobardo" as an alias. For example, his Uber account and one of his Facebook profiles was in the name "Leobardo Garcia." PATRON's co-conspirators also used "Leonardo" as an alias for PATRON. It is believed that "Leon" could be a shortened version of this alias. Finally, "Pw cloud: PatronLopez2323", appears to indicate that the iCloud password consists of PATRON's two family names (Patron Lopez.) Due to the aforementioned facts, I believe that **Subject Account** is controlled by PATRON.

E. Justification for Data and Date Range Sought

12. Please see the affidavit of Exhibit 1, specifically paragraphs 25-28.

*Applicability of the **Subject Accounts***

13. Please see the affidavit of Exhibit 1, specifically paragraphs 29-30.

INFORMATION REGARDING APPLE ID AND iCLOUD

14. Please see the affidavit of Exhibit 1, specifically paragraphs 31-45.

INFORMATION TO BE SEARCHED AND ITEMS TO BE SEIZED

15. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, FBI agents, or other federal agents, will review that information to locate the items described in Section II of Attachment B. The FBI issued a preservation letter for both accounts last week.

CONCLUSION

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

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

//

//

//

//

//

18. WHEREFORE, I request that the Court issue a warrant authorizing law enforcement agents and/or other federal and state law enforcement officers to seize and search the items described in Attachment A, and the seizure of items listed in Attachment B.

Jenna Paisley
Jenna Paisley
Special Agent
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 22nd day of November, 2024.

Allison H. Goddard
HON. ALLISON H. GODDARD
United States Magistrate Judge

Exhibit 1

UNITED STATES DISTRICT COURT

for the
SOUTHERN DISTRICT OF CALIFORNIA

NOT FOR PUBLIC VIEW

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

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A, incorporated herein by reference.

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before November 20, 2024
(not to exceed 14 days)

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge Benjamin J. Cheeks.
(name)

☐ The electronic communication service provider to whom this warrant is directed shall not notify any other person of the existence of this warrant until _____, absent further order of the Court, as the Court finds reason to believe that such notification will result in an adverse consequence as provided at 18 U.S.C. § 2705(b).

Date and time issued: 12:58 PM, Nov 6, 2024

Benjamin Cheeks
Judge's signature

City and state: San Diego, California

Hon. Benjamin J. Cheeks, United States Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT SOUTHERN DISTRICT OF CALIFORNIA

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing Officer's Signature

_____
Printed name and title

Print Form

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

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

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

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

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

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

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

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

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

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

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

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

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

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

III. Search of the Data

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

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

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

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

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

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

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

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

which are evidence of violations of 18 U.S.C. §§ 1203 (Conspiracy to take Hostages Resulting in Death), 21 U.S.C. §§ 848(e)(1)(A) (Intentional Killing While Engaged in Drug Trafficking), and Title 21 U.S.C. §§ 841 (Narcotics Trafficking).

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 hostgaes resultingin 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

AFFIDAVIT IN SUPPORT OF

APPLICATIONS FOR SEARCH WARRANTS

I, Jesse Crim, being duly sworn, state as follows:

INTRODUCTION

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with the following iCloud accounts:

a. Account 20298183955, e-mail address "patron_101026@hotmail.com" and believed to be used by Brian Alexis PATRON Lopez (**Subject Account 1**)

b. Account 11893452869, e-mail address "16deadpools@gmail.com" and believed to be used by Brian Alexis PATRON Lopez (**Subject Account 2**);

(Collectively, the **Subject Accounts**), between the dates of January 1, 2020 to present, for items which constitute evidence, fruits, and instrumentalities for violations of 18 U.S.C. §§ 1203 (Conspiracy to take Hostages Resulting in Death), 21 U.S.C. §§ 848(e)(1)(A) (Intentional Killing While Engaged in Drug Trafficking), and Title 21 U.S.C. §§ 841 (Narcotics Trafficking), (Collectively, the **Target Offenses**) as more fully described in Attachment B.

2. For the reasons set forth below, I believe there is probable cause for the requested warrant for the **Subject Accounts**, the contents of which are stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Apple Park Way, Cupertino, California 95014. The information to be disclosed by Apple and searched by the government is described in the

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

TRAINING & EXPERIENCE

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

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

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

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

FACTS IN SUPPORT OF PROBABLE CAUSE

A. Background of the Case

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

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

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

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

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

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

RENDON Steals Methamphetamine

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

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

[1] For context, the "document" is a reference to a Notice to Appear and seizure notice, 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.

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

RENDON is Kidnapped

12. On May 29, 2020, Rendon traveled to Tijuana from San Diego to a motel called "Motel El Parador."[2] MONTELLANO and an associate named Kenneth RIVERA learned from persons in contact with Rendon of Rendon's plans to travel to the Parador.

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

The Hostage Takers Contact RENDON's Family and Demand a Ransom

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

[2] "Motel El Parador" is located at Blvd. Cuauhtémoc Sur Pte. 405, Madero Sur, 22046 Tijuana, B.C., Mexico.

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

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

RENDON is murdered

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

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

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

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

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

B. Evidence Specific to Subject Accounts 1 and 2

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

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

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

a. Account 20298183955, with the email e-mail address "patron_101026@hotmail.com" (**Subject Account 1**)

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

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

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

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

E. Justification for Data and Date Range Sought

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

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

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

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

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

*Applicability of the **Subject Accounts***

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

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

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

INFORMATION REGARDING APPLE ID AND iCLOUD[3]

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

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

[3] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "iCloud: iCloud storage and 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.

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

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

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

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

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

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

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

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

33. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

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

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

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

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

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

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

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

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

a. Communications, photographs, videos, or other data depicting narcotics, plans or attempts to smuggle and traffic narcotics, narcotics proceeds,

b. Communications, photographs, videos, or other data depicting victims and targets of violent crimes, the planning or commission of violent crimes, and efforts to threaten victims or witnesses, collect ransoms, and elude law enforcement,

c. Internet and web-search history relating to narcotics trafficking and violent crimes;

d. Communications, photographs, videos, or other data shared with coconspirators to coordinate and then execute narcotics trafficking events and violent crimes, to include;

e. Celebratory remarks after the successful completion of a violent crime or narcotics trafficking event;

f. Geo-locational information related to a violent crime such as where it occurred and the location or remains of a victim during and after the commission of the crime;

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

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

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

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

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

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

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

INFORMATION TO BE SEARCHED AND ITEMS TO BE SEIZED

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

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

CONCLUSION

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

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

//

//

//

//

//

//

//

//

//

//

49. WHEREFORE, I request that the Court issue a warrant authorizing law enforcement agents and/or other federal and state law enforcement officers to seize and search the items described in Attachment A, and the seizure of items listed in Attachment B.

s/ Jesse Crim
Jesse Crim
Special Agent
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 6th day of November, 2024.

Benjamin Cheeks
HON. BENJAMIN J. CHEEKS
United States Magistrate Judge

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

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

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

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

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

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

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

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

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

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

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

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

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

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

III. Search of the Data

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

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

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

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

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

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

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

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

which are evidence of violations of 18 U.S.C. §§ 1203 (Conspiracy to take Hostages Resulting in Death), 21 U.S.C. §§ 848(e)(1)(A) (Intentional Killing While Engaged in Drug Trafficking), and Title 21 U.S.C. §§ 841 (Narcotics Trafficking).