UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

1850 Bradcliff Way, Palmdale, California 93551

Case No. 2:20-mj-04487-Duty

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-1

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

See Attachment B

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

☒ evidence of a crime;

☒ contraband, fruits of crime, or other items illegally possessed;

☒ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. §§ 841(a)(1), 846	Possession with Intent to Distribute a Controlled Substance and Conspiracy
21 U.S.C. §§ 843(b)	Use of a Communication Facility to Facilitate the Distribution of a Controlled Substance

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (*give exact ending date if more than 30 days*: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/
Applicant's signature

Christopher Siliciano, Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 b. telephone.

Date: September 18, 2020

Judge's signature

City and state: Los Angeles, CA

Hon. Michael R. Wilner, U.S. Magistrate Judge
Printed name and title

AUSA: Keith D. Ellison (213-894-6920) / Puneet V. Kakkar (213-894-5728)

ATTACHMENT A-1

PREMISES TO BE SEARCHED

The parcel located at 1850 Bradcliff Way, Palmdale, California 93551, containing a single family, two-story residence with light tan stucco walls with white trim. The front door is dark in color and located underneath a small porch facing north. The numbers “1850” are displayed the eve above the east side of the garage doors. The roof has light red tile shingles. The parcel is the second parcel east of 20th Street West on Bradcliff Way.

The area to be searched includes all rooms, annexes, attics, basements, porches, garages, carports, outside yard, curtilage, mailboxes, trash containers, debris boxes, storage lockers, locked containers and safes, cabinets, rooms, parked vehicles, motorhomes, sheds, and outbuildings associated with the premises and shall extend into desks, cabinets, safes, briefcases, backpacks, wallets, purses, trash receptacles, digital devices, and any other storage locations within the premises.

ATTACHMENT B

ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 21 U.S.C. §§ 841(a)(1) (Manufacturing, Distribution of, and Possession with Intent to Distribute, a Controlled Substance), 846 (Attempt and Conspiracy to Commit Controlled Substance Offense), and 843(b) (Unlawful Use of a Communication Facility, Including the Mails, to Facilitate the Distribution of a Controlled Substance) (the "Subject Offenses"):

a. Any controlled substance, controlled substance analogue, or listed chemical;

b. Firearms, ammunition, silencers, and other dangerous weapons;

c. Items and paraphernalia for the manufacturing, distributing, packaging, sale, or weighing of controlled substances, including scales and other weighing devices, plastic baggies, food saver sealing devices, heat sealing devices, balloons, packaging materials, containers, and money counters;

d. United States currency in excess of $2,000, including the first $2,000 if more than $2,000 is seized, digital currency such as Bitcoin stored on electronic wallets or other forms of wallets or other means, cryptocurrency private keys and recovery seed, and records relating to income derived from the transportation, sales, and distribution of controlled substances and expenditures of money and wealth, for example, money orders, wire transfers, cashier's checks and receipts,

passbooks, cash cards, gift cards, checkbooks, check registers, securities, precious metals including gold, jewelry, antique or modem automobiles, bank statements and other financial instruments, including stocks or bonds in amounts indicative of the proceeds of illicit narcotic trafficking;

e. Records, documents, programs, applications and materials reflecting the identity of, contact information for, communications with, or times, dates or locations of meetings with co-conspirators, sources of supply of controlled substances, or drug customers, including calendars, address books, telephone or other contact lists, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times when drugs were bought, sold, or otherwise distributed, whether contained in hard copy correspondence, notes, emails, text messages, photographs, videos (including items stored on digital devices), or otherwise;

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

g. Storage units and containers, such as floor safes, wall safes, upright safes (also known as gun safes), lock boxes, and other self-contained locked enclosures;

h. Records, documents, programs, applications and materials indicating travel in interstate and foreign commerce, such as travel itineraries, plane tickets, boarding passes,

motel and hotel receipts, passports and visas, credit card receipts, and telephone bills

i. Indicia of occupancy, residency, and/or ownership of the previously described property, premises, or vehicles, and any other property, premises, or vehicles, including utility and telephone bills, canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, envelopes, registration, receipts, and keys which tend to show the identities of the occupants, residents, and/or owners; and

j. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.

2. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

b. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the attachment of other devices;

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

e. evidence of the times the device was used;

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

g. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

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

i. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

3. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

4. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as

telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

SEARCH PROCEDURE FOR DIGITAL DEVICE(S)

5. In searching digital devices (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

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

6. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

7. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the

government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

8. During the execution of this search warrant, law enforcement is permitted to: (1) depress BERMUDEZ's thumb- and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of BERMUDEZ's face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

9. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, Christopher Siliciano, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint and arrest warrant against ANDRES BERMUDEZ, also known as "Tito" ("BERMUDEZ"), for a violation of 21 U.S.C. §§ 841(a)(1), (b)(1)(A)(viii): Possession with Intent to Distribute a Controlled Substance.

2. This affidavit is also made in support of an application for a warrant to search the following:

a. 1850 Bradcliff Way, Palmdale, California 93551 (the "**Subject Premises**"), as described more fully in Attachment A-1;

b. A Honda Civic, California license plate number 7UVU643, registered to Moises A. Castro ("**Subject Vehicle 1**"), as described more fully in Attachment A-2;

c. A motorhome, California license plate number 4PTY764, registered to Kristina Baca ("**Subject Vehicle 2**" and, collectively with **Subject Vehicle 1**, the "**Subject Vehicles**"), as described more fully in Attachment A-3; and

d. The person of BERMUDEZ, as further described in Attachment A-4.

3. The requested search warrant seeks authorization to seize evidence, fruits, or instrumentalities of violations of 21 U.S.C. §§ 841(a)(1) (Manufacturing, Distribution of, and Possession with Intent to Distribute, a Controlled Substance), 846 (Attempt and Conspiracy to Commit Controlled Substance

Offense), and 843(b) (Unlawful Use of a Communication Facility, Including the Mails, to Facilitate the Distribution of a Controlled Substance) (the "Subject Offenses"), as described more fully in Attachment B. Attachments A-1, A-2, A-3, A-4, and B are incorporated herein by reference.

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

II. BACKGROUND OF AFFIANT

5. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed since October 2017. As a requirement for employment as an FBI Special Agent, I successfully completed the New Agent Basic Field Training Course located at the FBI Training Academy in Quantico, Virginia. As a function of my assignment, I have received both formal and informal training from the FBI and other institutions regarding computer technology, financial investigations, cryptocurrency, and drug trafficking organizations.

6. As a Special Agent with FBI, part of my duties includes the investigation of criminal violations as proscribed by 21 U.S.C § 841 and 21 U.S.C § 846. Moreover, as an FBI

Special Agent, I am a Federal Law Enforcement Officer, authorized to investigate violations of the laws of the United States and to execute search and seizure warrants issued under the authority of the United States.

7. I have conducted and participated in criminal investigations for violations of federal and state laws including, but not limited to, narcotics trafficking, computer-based financial crimes, money laundering, firearms, fraud, and other organized criminal activity. I have prepared, executed, and assisted in numerous search and arrest warrants. I have also conducted and participated in criminal and administrative interviews of witnesses and suspects. I am familiar with the formal methods of illegal narcotics investigations, including, but not limited to, electronic surveillance, visual surveillance, general questioning of witnesses, search warrants, confidential informants, the use of undercover agents, and analysis of financial records. I have participated in investigations of organizations involved in the manufacture, distribution, and possession with intent to distribute controlled substances, including those involving the dark web and virtual currency.

III. SUMMARY OF PROBABLE CAUSE

8. Since February 2019, the FBI, Homeland Security Investigations ("HSI"), and United States Postal Inspection Service ("USPIS") have been investigating a drug trafficking organization (the "STEALTHGOD DTO") selling narcotics, including methamphetamine and 3, 4-Methylenedioxymethamphetamine ("MDMA")

on darknet marketplaces suspected of operating the monikers "Hectorsmom", "Stealthgod", and others. In February 2020, law enforcement arrested five individuals in connection with this DTO and after searching two residences used in furtherance of the criminal scheme, seized approximately 120 pounds of methamphetamine, 30,000 pills of suspected MDMA, and five firearms. Based on further investigation from that search, agents have identified BERMUDEZ as one of the sources of supply of methamphetamine to the STEALTHGOD DTO. BERMUDEZ has resided at the **Subject Premises** and has been observed driving the **Subject Vehicles**. Based on the training and experience of investigators, evidence of drug trafficking is expected to be recovered from the **Subject Premises** and the **Subject Vehicles**.

IV. BACKGROUND ON DARKNET DRUG TRAFFICKING

9. Based on my training and experience, I am aware of the following concepts:

a. The "dark web," also sometimes called the "dark net" or "deep web," is a colloquial name for a number of extensive, sophisticated, and widely used criminal marketplaces operating on the Internet, which allow participants to buy and sell illegal items, such as drugs, firearms, and other hazardous materials with greater anonymity than is possible on the traditional Internet (sometimes called the "clear web" or simply "web"). These online black market websites use a variety of technologies, including the Tor network (defined below) and other encryption technologies, to ensure that communications and transactions are shielded from interception and monitoring. A

famous dark web marketplace, Wall Street Market, operated similar to legitimate commercial websites such as Amazon and eBay, but offered illicit goods and services. Law enforcement shut down Wall Street Market in 2019.

b. "Vendors" are the dark web's sellers of goods and services, often of an illicit nature, and they do so through the creation and operation of "vendor accounts."

c. The "Tor network," or simply "Tor," is a special network of computers on the Internet, distributed around the world, that is designed to conceal the true Internet Protocol ("IP") addresses of the computers accessing the network, and, thereby, the locations and identities of the network's users. Tor likewise enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites, which are referred to as "hidden services" on the Tor network. Such "hidden services" operating on Tor have complex web addresses, generated by a computer algorithm, ending in ".onion" and can only be accessed through specific web browser software, including a major dark-web browser known as "Tor Browser," designed to access the Tor network. One of the logos, or "icons," for Tor Browser is a simple image of the Earth with purple water and bright green landmasses with bright green concentric circles wrapping around the planet to look like an onion.

d. Darknet marketplaces often only accept payment through virtual currencies, such as Bitcoin, and operate an escrow whereby customers provide the digital currency to the

marketplace, who in turn provides it to the vendor after a transaction is completed. Accordingly, large amounts of Bitcoin sales or purchases by an individual can be an indicator that the individual is involved in drug trafficking or the distribution of other illegal items. Individuals intending to purchase illegal items on Wall Street Market-like websites need to purchase or barter for Bitcoins.

e. When vendors receive orders for narcotics on the darknet, the orders can come from anywhere in the world; vendors are known to use U.S. mail and/or commercial carriers to distribute narcotics.

f. Vendors operate akin to traditional drug trafficking organizations, with sources of supply (who provide drugs to them) and couriers (who drop off mail packages to customers).

V. STATEMENT OF PROBABLE CAUSE

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

A. Background of Investigation

11. Since February 2019, federal law enforcement agents have been investigating a group of darknet drug vendors believed to be operated by the same group, including "HectorsMom" and "Stealthgod," which collectively made over 18,000 sales on the darknet. These vendor monikers sold drugs on a variety of darknet marketplaces (some of which are now defunct), such as Wall Street Market, Empire, and Nightmare, and through encrypted

communications platforms such as ProtonMail. Over the course of the investigation, these vendors sold methamphetamine for approximately $400 per ounce. Agents believed that these monikers were affiliated with each other based on the advertisements and comments on darknet forums. Agents conducted undercover purchases of drugs, including methamphetamine, from some of these vendor monikers. These vendors sent drugs hidden in items such as puzzle boxes and health and wellness products.

B. February 11, 2020, Drug Seizures

12. In connection with this investigation, on February 10, 2020, the Honorable Jacqueline Chooljian, United States Magistrate Judge, authorized search warrants for two locations in the Central District of California associated with the STEALTHGOD DTO, specifically the residence of Rane Melkom and Teresa McGrath (the "Scoville Residence") and a residence occupied by Mark Chavez, Thomas Olayvar, and Matthew Ick ("the "Stoa Residence"). Law enforcement officers executed the warrants on February 11, 2020.

13. During the search of the Scoville Residence, Melkom and McGrath were present;[1] law enforcement officers found the following in a shed adjoining the residence:

[1] Melkom and McGrath have been charged in a two-count information for possession with intent to distribute methamphetamine and MDMA, in violation of 21 U.S.C. §§ 841(a)(1), (b)(1)(A)(viii), (b)(1)(C). McGrath has pleaded guilty to a superseding information charging her with conspiracy to distribute and posses with intent to distribute methamphetamine and MDMA, in violation of 21 U.S.C. §§ 841(a)(1), (b)(1)(A)(viii), (b)(1)(C), conspiracy to launder monetary instruments, in violation of 18 U.S.C. § 1956(h), and

a. 22.183 kilograms of actual methamphetamine.

b. Approximately 6,701 grams of MDMA.

c. Two loaded Glock pistols, bearing serial numbers NRU539 and GMZ799.

d. 60 packaged and sealed USPS priority mail envelopes addressed to various addresses, in over 35 states across the country, that were later discovered to contain drugs, including a crystalline like substance that yielded a presumptive positive for the presence of methamphetamine, orange triangle and square shaped pills that yielded a presumptive positive for the presence of MDMA, Orange circle shaped pills marked “AD30” that yielded a presumptive positive for the presence of methamphetamine, a brown tar-like substance suspected to be hashish, and white rectangular pills suspected to be Alprazolam.

14. In addition, in the residence portion of the Scoville Residence, law enforcement officers seized a loaded FNH pistol, bearing serial number GKU0127246, under the bed of Melkom and McGrath.

15. During the search of the Stoa Residence, Chavez, Olayvar, Ick, and others were present;[2] law enforcement officers found the following:

---

possession of firearms in furtherance of drug trafficking, in violation of 18 U.S.C. § 924(c). See United States v. Melkom and McGrath, 20-CR-00136-AB.

[2] Chavez has pleaded guilty to an information charging him with conspiracy to possess with intent to distribute and distribute methamphetamine and MDMA, in violation of 21 U.S.C. §§ 841(a)(1), (b)(1)(A)(viii), (b)(1)(C) and possession of

a. Approximately 16.62 kilograms (36.64 pounds) of methamphetamine; and

b. Two loaded handguns.

C. Review of Surveillance Video of Scoville Residence Identifies Chavez Supplying Melkom With Drugs

16. During the search of Melkom's residence described above, agents identified a surveillance camera installed over the entry of the shed at the Scoville Residence, where the drugs were discovered.

17. On August 5, 2020, the Honorable Pedro V. Castillo, United States Magistrate Judge, Central District of California, authorized a warrant for the production and search of information -- including video recordings -- associated with the camera held with the provider of that surveillance camera.

18. During my review of video recordings obtained pursuant to the warrant, I observed a video from February 9, 2020, showing Melkom and Chavez carrying black duffel bags from a car into the portion of Melkom's residence where the drugs were discovered. Based on my training, experience, and investigation in this case, I believe that Chavez delivered methamphetamine to Melkom for further distribution via the dark web.

---

firearms in furtherance of drug trafficking, in violation of 18 U.S.C. § 924(c). See United States v. Chavez, 20-CR-00130-AB. Olayvar and Ick are currently charged in an information with possession with intent to distribute methamphetamine in violation of 21 U.S.C. §§ 841(a)(1), (b)(1)(A)(viii). See United States v. Olayvar and Ick, 20-CR-00135-AB.

D. Search of Chavez's Phone Reveals Identity of BERMUDEZ Involved With Supplying Chavez With Methamphetamine

19. Agents lawfully searched Chavez's cellular telephone that was seized from the Stoa Residence, which was an iPhone with phone number ending in 8606 (the "Chavez phone"). During a search of the Chavez phone, I found messages whereby Chavez used coded language to discuss purchasing bulk amounts of drugs from several individuals. Relevant here, I found several messages between the Chavez phone and a phone number ending in 8004 (the "BERMUDEZ phone"), to include the following:

a. On January 18, 2020, the BERMUDEZ phone sent a message to Chavez stating: "Hey mark there 50 real good right here at my boys house this is one of my good boys his well connect I've been talking him about having 50 to 100 sitting there just for u so he has them let me know".

i. Based on my background, training, experience, and investigation in this case, I believe that Chavez and the BERMUDEZ phone were discussing methamphetamine transactions in terms of pounds of product, such that "50 to 100" means 50 to 100 pounds of methamphetamine.

b. On February 7, 2020, the BERMUDEZ phone sent a message to Chavez stating: "Hey mark How are you Everything good I was Calling you to let you know I could get you some real good ones nice and chunky for a good price as many as need 30lb + for $975."

i. Based on my training and experience, I know drug traffickers describe quality methamphetamine using terms

like “chunky”. Based on my background, training, experience, and investigation in this case, I believe that Chavez and the BERMUDEZ phone were again discussing methamphetamine transactions.

c. Between February 9 and 10, 2020, Chavez and the BERMUDEZ phone exchanged the following messages:

Chavez:	Hay buddy I need another 30
BERMUDEZ phone:	Okay Let me see
Chavez:	Can you try to get at 950 brother
BERMUDEZ phone:	Yo what’s good mark , my boy just called me he said there’s gonna be 200 of them around 4:30-5:00pm let me know how many u want so he could put them to side
Chavez:	Yes I’ll be ready at 8

i. Based on my background, training, experience, and investigation in this case, I believe that Chavez and the user of the BERMUDEZ phone were negotiating the sale of 30 pounds of methamphetamine (“another 30”) for $950 per pound (“Can you try to get at 950 brother”).

d. During a search of the Chavez phone, I also found messages to and from Melkom discussing the acquisition, and delivery to Melkom’s residence, of large quantities of methamphetamine.[3] Relevant here, on February 10, 2020, at 11:03 p.m., Chavez sent a message to Melkom stating, “Okay I got another 40.”

[3] Agents have also lawfully searched Melkom’s phone that was seized in connection with the above-referenced search warrants and have identified the corresponding messages in that phone.

i. Based on my background, training, experience, and investigation in this case, I believe that Chavez messaged Melkom to tell Melkom he had obtained an additional 40 pounds of methamphetamine ("I got another 40"). I further believe, based on the context of this message, that this was the approximately 40 pounds that investigators seized from the Stoa residence on February 11, 2020.

E. Review of Cell-Site Information Reflects Chavez and BERMUDEZ Met Before February 11, 2020 in a Suspected Drug Transaction

20. On January 30, 2020, the Honorable Alexander F. MacKinnon, United States Magistrate Judge, authorized a continued warrant for the disclosure of prospective cell-site and GPS information for the Chavez phone. On March 10, 2020, the Honorable John E. McDermott, United States Magistrate Judge, authorized a warrant for the disclosure of historical cell-site information and prospective cell-site and GPS information for the BERMUDEZ phone.

21. Based on my review of the cell-site and GPS information obtained pursuant to the warrants, I am aware that the Chavez phone and the BERMUDEZ phone were both located in the vicinity of east Los Angeles around the same time -- between 10:00 and 10:30 p.m. -- on the evening of February 10, 2020. Information for the location of the Chavez phone reflects that Chavez did not regularly spend time in that area.

22. Based on my review of messages on the Chavez phone, the cell-site information, the surveillance video, and my investigation in this case, I believe that on February 10, 2020,

the user of the BERMUDEZ phone provided Chavez with the approximately 40 pounds of methamphetamine seized from Chavez's residence on February 11, 2020. I further believe that Chavez obtained the drugs in connection with Melkom for sale on the dark web.

F. Deputies Arrest BERMUDEZ with Methamphetamine in March 2020

23. On March 28, 2020, unrelated to the investigation described above, Los Angeles County Sheriff's Department ("LASD") deputies conducted a traffic stop of **Subject Vehicle 1** for a moving violation on Soledad Canyon Road in Canyon Country, California. Based on my review of that report, I am aware of the following:

a. During the stop, deputies identified the driver as BERMUDEZ. Deputies saw drug paraphernalia in plain view and inquired whether there was anything else illegal in the vehicle, to which BERMUDEZ responded he had methamphetamine inside. Deputies conducted a search of the vehicle and found suspected methamphetamine in a Ziploc bag stuffed between the driver's seat and center console. Deputies also recovered a plastic baggie containing a black, tar-like substance resembling heroin in the center console.

b. After the deputies advised BERMUDEZ of his Miranda rights, which he appeared to understand and agreed to waive, BERMUDEZ stated the drugs belonged to him but denied selling drugs.

c. The deputies arrested BERMUDEZ on charges of possession of a controlled substance (methamphetamine) for sale, possession of heroin, and possession of drug paraphernalia. He was booked at the Los Angeles Sheriff's Santa Clarita Station, and subsequently released from custody.

d. At the time of his arrest, BERMUDEZ provided officers with his address (the **Subject Premises**) and phone number (the BERMUDEZ phone).

24. Forensic chemists at the DEA Southwest Laboratory later confirmed the suspected methamphetamine to be 58 grams of methamphetamine hydrochloride.

25. A review of the cell-site and GPS information for the BERMUDEZ phone at the time of the traffic stop and subsequent arrest, places the BERMUDEZ phone in the vicinity of Soledad Canyon Road, and, later, the Los Angeles County Sheriff's Department Santa Clarita Station. Based on this information, I believe that BERMUDEZ is the user of the BERMUDEZ phone.

G. Additional Surveillance of BERMUDEZ

26. As discussed above, at the time of his arrest, BERMUDEZ provided officers with his address (the **Subject Premises**) and phone number (the BERMUDEZ phone).

27. On April 14, 2020, an LASD detective conducted surveillance at 42524 3rd Street, East Lancaster, California, based on location information received from the BERMUDEZ phone. **Subject Vehicle 2** was observed parked on the west shoulder of 3rd Street east across from 42534 3rd St. East.

28. On April 21, 2020, an LASD detective received a location "ping" for the BERMUDEZ phone to a location near 3rd Street East and Avenue L-4 in Lancaster, California. The LASD Detective observed **Subject Vehicle 1** and **Subject Vehicle 2** parked next to each other in the location of the phone ping. **Subject Vehicle 2** had interior lights illuminating the rear portion of the motorhome.

29. On April 28, 2020, an LASD detective reviewing cell-site and GPS information for the BERMUDEZ phone tracked the phone's location to the vicinity of the **Subject Premises.** Later that day, the detective conducted surveillance of the **Subject Premises** and saw **Subject Vehicle 1** parked in front of the residence.

30. On April 29, 2020, at the request of the LASD detective, an LASD deputy stopped **Subject Vehicle 1** in Palmdale, California, for a tinted windows violation. The deputy identified BERMUDEZ as the sole occupant of the vehicle and observed that he was exhibiting signs and symptoms of recent drug use. After BERMUDEZ told the deputy that he had recently used narcotics, the deputy detained BERMUDEZ in the back seat of the patrol car pending a narcotics investigation. During the course of the investigation, the LASD detective (who has assisted with this investigation, as described above) arrived and confirmed BERMUDEZ was the driver of **Subject Vehicle 1**. The detective also called the BERMUDEZ phone while the detective was at the location. The deputy saw the phone in BERMUDEZ's possession light up, and heard it ring, when the detective

called. The deputy provided BERMUDEZ with a warning and released him.

31. The detective later reviewed cell-site and GPS information for the BERMUDEZ phone around the time of the traffic stop and saw that the phone appeared at the location of the traffic stop during that time. Following the stop, cell-site and GPS information for the BERMUDEZ phone show that BERMUDEZ went directly to the vicinity of the **Subject Premises.**

32. On May 1, 2020, the detective conducted surveillance of the **Subject Premises**. At 5:50 a.m., the detective saw **Subject Vehicle 1** parked in front of the residence. At 5:00 p.m., the detective saw BERMUDEZ sitting in a chair on the front porch of the **Subject Premises**.

33. Based on my review of cell-site and GPS information for the BERMUDEZ phone, I am aware that the BERMUDEZ phone -- and, thus, BERMUDEZ -- is regularly in the vicinity of the **Subject Premises.** When he is not at the **Subject Premises**, BERMUDEZ commonly drives to Santa Clarita, San Fernando, North Hollywood, Van Nuys, or Sunland. Cell-site and GPS information show that BERMUDEZ stops at various stores and gas stations while in those areas. Based on my knowledge of this investigation, I believe that BERMUDEZ transports controlled substances from the **Subject Premises** to those areas for the purpose of sales.

34. On September 9, 2020, the Honorable Patricia Donahue, United States Magistrate Judge, authorized a renewed warrant for the disclosure of historical cell-site information and

prospective cell-site and GPS information for the BERMUDEZ phone. Based on a review of this historical cell-site information, I learned the following:

a. On July 28, 2020, the BERMUDEZ phone made multiple outgoing phone calls. The first tower to receive a signal from the BERMUDEZ phone during these calls placed the address of this phone call nearby 38650 5th Street West, Palmdale, California 93551, in the general vicinity of the **Subject Premises.**

b. The BERMUDEZ phone has made multiple outgoing calls in Sherman Oaks, California, as recently as September 1, 2020.

35. On September 17, 2020, I observed the **Subject Vehicles** parked together in the vicinity of 5225 Sepulveda Blvd., Sherman Oaks, California 91411. The vehicles were attached, and appeared to have been parked in that location consistently. Based on the location of the vehicles, I believe that BERMUDEZ is spending consistent time living in **Subject Vehicle 2.**

Photo from September 16, 2020:

VI. TRAINING AND EXPERIENCE ON DRUG OFFENSES

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

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

b. Drug traffickers often maintain books, receipts, notes, ledgers, bank records, and other records relating to the manufacture, transportation, ordering, sale and distribution of illegal drugs, including for historical transactions. The aforementioned records are often maintained where drug traffickers have ready access to them, such as on their cell phones and other digital devices, and in their residences and vehicles. These records are also maintained after a sale has occurred.

c. Communications between people buying and selling drugs take place by telephone calls and messages, such as e-mail, text messages, and social media messaging applications, sent to and from cell phones and other digital devices. This includes sending photos or videos of the drugs between the seller and the buyer, the negotiation of price, and discussion

of whether or not participants will bring weapons to a deal. In addition, it is common for people engaged in drug trafficking to have photos and videos on their cell phones of drugs they or others working with them possess, as they frequently send these photos to each other and others to boast about the drugs or facilitate drug sales.

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

e. Drug traffickers often use vehicles to transport their narcotics and may keep stashes of narcotics in their vehicles in the event of an unexpected opportunity to sell narcotics arises.

f. Drug traffickers often maintain on hand large amounts of United States currency in order to maintain and finance their ongoing drug trafficking businesses, which operate on a cash basis. Such currency is often stored in their residences and vehicles.

g. Drug traffickers often keep drugs in places where they have ready access and control, such as at their residence or in safes. They also often keep other items related to their drug trafficking activities at their residence, such as digital scales, packaging materials, and proceeds of drug trafficking. These items are often small enough to be easily hidden and thus

may be kept at a drug trafficker's residence even if the drug trafficker lives with others who may be unaware of his criminal activity.

h. It is common for drug traffickers to own multiple phones of varying sophistication and cost as a method to diversify communications between various customers and suppliers. These phones range from sophisticated smart phones using digital communications applications such as Blackberry Messenger, WhatsApp, and the like, to cheap, simple, and often prepaid flip phones, known colloquially as "drop phones," for actual voice communications.

i. When drug traffickers deal with significant quantities of drugs, such as methamphetamine, they may also possess firearms for protection of those drugs. That appeared to be the case with respect to the STEALTHGOD DTO, given that both residences where significant quantities of methamphetamine was found also had guns found in the proximity of the drugs.

VII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[4]

37. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I

[4] As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

know that the following electronic evidence, inter alia, is often retrievable from digital devices:

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

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

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

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

38. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

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

39. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an

enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress BERMUDEZ's thumb- and/or fingers on the device(s); and (2) hold the device(s) in front of BERMUDEZ's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

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

VIII. CONCLUSION

41. For all of the reasons described above, there is probable cause to believe that BERMUDEZ has committed a violation of 21 U.S.C. § 841(a)(1), (b)(1)(A)(viii): Possession with Intent to Distribute a Controlled Substance. There is also probable cause to believe that the items to be seized described in Attachment B will be found in a search of the **Subject Premises**, the **Subject Vehicles**, and the person of BERMUDEZ as further described above and in the various Attachments A.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 18th day of September, 2020.

UNITED STATES MAGISTRATE JUDGE

Hon. Michael R. Wilner