AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America

v.

Andrew Madi,

Defendant(s)

Case No. 18-MJ

MJ 18-3188

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of July 3, 2018 in the county of Los Angeles in the Central District of California, the defendant(s) violated:

Code Section	*Offense Description*
21 U.S.C. §§ 841(a)(1), (b)(1)(C)	Distribution of fentanyl resulting in death

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

Complainant's signature

Charles Valentine, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 11/30/18

Judge's signature

City and state: Los Angeles, California

Hon. ~~Karen L. Stevenson~~, U.S. Magistrate Judge

Printed name and title

PATRICK J. WALSH

KB

AFFIDAVIT

I, Charles Valentine, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint against Andrew MADI ("MADI") for a violation of Title 21, United States Code, Sections 841(a)(1), (b)(1)(C) (distribution of fentanyl resulting in death), namely, that on or about July 3, 2018, in Los Angeles County, within the Central District of California, MADI knowingly and intentionally distributed fentanyl, a Schedule II narcotic drug controlled substance, to Alex Gertsch, a 25-year-old male whose death and serious bodily injury resulted from the use of such substance.

2. As set forth in more detail below, MADI was arrested on November 30, 2018, following execution of federal search warrants (18-MJ-3158 and 18-MJ-3159) at MADI's places of residence earlier that day. A copy of the search warrant and supporting affidavit in matter 18-MJ-3158 an excerpted copy of which is attached hereto as Attachment A. Attachment A is incorporated as though fully set forth herein.

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint 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. INTRODUCTION

4. I am an investigative and law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), and I am empowered by law to conduct investigations of, and to make arrests for, the offenses enumerated in Title 18, United States Code, Section 2516. I am currently a Special Agent ("SA") with the Drug Enforcement Administration ("DEA"), Los Angeles Field Division Enforcement Group 4. I have been employed as a DEA SA since September 2012.

5. My training and experience is described in more detail at paragraphs 2 through 4 of Attachment A, which as noted are incorporated herein.

III. STATEMENT OF PROBABLE CAUSE

6. On November 29, 2018, the Hon. Paul L. Abrams, United States Magistrate Judge, signed search warrants in matters 18-MJ-3158 and 18-MJ-3159 authorizing the search of two residents used by MADI, namely, 855 North McCadden Place, Los Angeles, California ("SUBJECT LOCATION 1") and the residence located at 115 South Commonwealth Avenue, Los Angeles, California. ("SUBJECT LOCATION 2" and collectively the "SUBJECT LOCATIONS"). Both warrants were based on an identical supporting affidavit, a copy of which is included in Attachment A.

7. I submit that the Probable Cause section set forth in Attachment A at paragraphs 8 through 36 establishes probable cause that MADI committed the offense underlying this complaint,

namely, that MADI knowingly and intentionally sold fentanyl to Gertsch on or about July 3, 2018, the use of which caused Gertsch to suffer a fatal overdose.

8. During the search of SUBJECT LOCATIONS, investigators seized, among other thing, small quantities of suspected heroin and suspected controlled drug pills, and various digital items for which forensic examination is pending. MADI was present at SUBJECT LOCATION 1 and, after waiving his Miranda rights, submitted to an interview conducted by myself and two other agents. I believe that MADI made false statements during the interview. For example, MADI denied that he sold drugs via Craigslist, but after agents confronted him with some of the evidence against him in this matter, MADI ultimately admitted that he has in fact sold heroin and "china white" via Craigslist, including during summer 2018 (i.e., during the timeframe in which he sold fentanyl to Gertsch that caused him to suffer a fatal overdose). MADI also denied using the dark web to purchase controlled drug stock, which I also believe is false for the reasons set forth in Attachment A. I showed MADI copies of the text messages of his exchange with Gertsch coordinating the July 2018 transaction, and MADI denied that he sent them, although here again I submit that he lied in doing so for the reasons set forth in Attachment A. Based on what I perceived to be MADI's false and minimized statements, and my determination that MADI either could not or would not provide valuable cooperation, agents arrested MADI in anticipation of obtaining the underlying complaint.

IV. CONCLUSION

9. For all the reasons described above, there is probable cause to believe that MADI has committed a violation of Title 21, United States Code, Sections 841(a)(1), (b)(1)(C) (distribution of fentanyl resulting in death), as described further in paragraph 1 above.

Charles Valentine
Special Agent
Drug Enforcement Administration

Subscribed to and sworn before me
this 30th day of November, 2018.

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

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)* 855 North McCadden Place Los Angeles, CA 90038	)	Case No. 2:18-MJ-03158

APPLICATION FOR A SEARCH WARRANT

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*
See Attachment B	

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.

Applicant's signature

DEA Special Agent Charles Valentine

Printed name and title

Sworn to before me and signed in my presence.

Date: 11/29/18

Judge's signature

City and state: Los Angeles, CA

Hon. Paul L. Abrams, United States Magistrate Judge

Printed name and title

AUSA: Benjamin Barron (ext. 3542)

ATTACHMENT A

AFFIDAVIT

I, Charles Valentine, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am an investigative and law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), and I am empowered by law to conduct investigations of, and to make arrests for, the offenses enumerated in Title 18, United States Code, Section 2516. I am currently a Special Agent ("SA") with the Drug Enforcement Administration ("DEA"), Los Angeles Field Division Enforcement Group 4. I have been employed as a DEA SA since September 2012.

2. Prior to my employment with the DEA, I was a police officer with the Oskaloosa, Iowa Police Department ("OPD") from approximately January, 2003, where I performed routine patrol activities and conducted drug investigations. During my time as a police officer for the City of Oskaloosa, I graduated from the 193rd Basic Iowa Law Enforcement Academy where I learned basic investigative skills including drug investigations and drug identification. During my time as a police officer, I conducted and assisted in various investigations including but not limited to drug investigations, burglaries, theft/fraud (including prescription fraud), assaults, drunk driving, and general complaints. I was assigned as a detective to the Mahaska County Drug Task Force in January of 2007 where I conducted drug investigations in and around Mahaska County, Iowa. As a drug investigator, I initiated and assisted in numerous

investigations involving the use, distribution, and manufacture of illegal drugs. I have also initiated and participated in investigations involving conspiracies to manufacture methamphetamine, conspiracies to distribute methamphetamine and/or marijuana, and conspiracies to illegally distribute pharmaceutical drugs. I was certified to conduct investigations involving hazardous materials found in clandestine methamphetamine laboratories, and have conducted multiple investigations into the manufacture of methamphetamine.

3. During the course of my employment with DEA, I have received several hundred hours of comprehensive, formalized instruction to include such topics as drug identification; money laundering techniques; patterns of drug trafficking; complex conspiracies; the exploitation of drug traffickers' telecommunications devices; criminal law; surveillance; and other investigative techniques. I have assisted in numerous investigations into the unlawful importation, manufacture, possession with intent to distribute, and distribution of controlled substances, the laundering of drug proceeds, and conspiracies associated with drug offenses. In conducting these investigations, I have utilized a variety of investigative techniques and resources, including but not limited to such techniques as surveillance, confidential source debriefings, telephone toll analysis, and wire communications analysis in other Title III wiretap investigations.

4. Through these investigations, my training and experience, and conversations with federal and state law

enforcement investigators, I have become familiar with the methods used by drug traffickers to smuggle and safeguard drugs, to distribute drugs, and to collect and launder proceeds related to the sales of drugs. I am familiar with methods employed by large-scale drug organizations, and the sophisticated tactics that they routinely use in attempts to thwart the investigation of their drug organizations, including the utilization of cellular telephone (and smartphone) technology, counter surveillance techniques, debit calling cards, public telephones, hidden vehicle compartments, elaborately planned smuggling schemes tied to legitimate businesses, false or fictitious identities, and coded communications and conversations. The facts set forth below are based upon (1) my own personal observations; (2) reports and information provided to me by other law enforcement agents or government agencies; (3) other documents obtained during the course of the investigation; and (4) evidence cultivated through other search warrants related to this investigation.

II. PURPOSE OF AFFIDAVIT

5. I make this affidavit in support of an application for a warrant to search the residence located at 855 North McCadden Place, Los Angeles, California ("SUBJECT LOCATION 1") and the residence located at 115 South Commonwealth Avenue, Los Angeles, California. ("SUBJECT LOCATION 2" and collectively the "SUBJECT LOCATIONS"), which are both fully described in Attachments A(1) and A(2) hereto.

ATTACHMENT A

6. As described more fully below, I respectfully submit there is probable cause to believe that information, evidence, contraband, fruits, or instrumentalities of criminal violations of 21 U.S.C. § 841(a)(1), (b)(1)(C) (distribution of controlled substances, including distribution resulting in death), 21 U.S.C. § 843(c) (advertising the sale of controlled substances via the internet), and 18 U.S.C. § 1956 (money laundering) are contained within the SUBJECT LOCATIONS, as further described in Attachment B hereto. Attachments A(1), A(2), and B are incorporated as though fully set forth herein.

7. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested 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.

III. STATEMENT OF PROBABLE CAUSE

8. I am investigating the drug overdose death of victim A.G., which occurred sometime between July 4, 2018 and July 6, 2018, the latter of which is when A.G. was found deceased in his apartment by his family members.

9. The Los Angeles County Coroner's office conducted an investigation into the cause of death and concluded that A.G. died from acute fentanyl toxicity, that is, from a fentanyl

overdose. From my training and experience, I know that fentanyl is a synthetic opioid that is approximately 50 times more powerful than heroin. I have spoken with coroner's investigator Ricardo Lopez, who informed me that on investigating the scene of A.G.'s death, he found inside a backpack in A.G.'s bedroom a smoking instrument that bore apparent residue and a baggie containing a white powdery substance. I retrieved those items from the Los Angeles County Coroner's Office and submitted them to the DEA Southwest Laboratory for chemical analysis. The analysis concluded that the baggie contained .3202 grams of fentanyl and that the foil contained fentanyl residue. The items were also submitted for fingerprint analysis, but no usable latent fingerprints could be recovered from them.

1. Drug Transaction on July 3, 2018

10. A.G.'s family has been assisting the DEA, including by providing access to A.G.'s cellular telephone. Forensic review of A.G.'s cellular telephone shows that, on or about July 3 and 4, 2018, A.G. viewed multiple postings on Craigslist advertising the sale of "roofing tar," which I recognize to be code for heroin (e.g., black tar heroin). In the same approximate timeframe, A.G. also ran Google searches such as "found heroin on craigslist;" "found drugs on craigslist;" "Craigslist as a source for heroin;" "china white cut with fentanyl" (I know "china white" to be common slang for fentanyl or heroin mixed with fentanyl); "overdose smoking heroin;" and "smoking china white." A.G. also viewed an article entitled "Drugs Decoded - Street Names for Drugs and Common Code Words Teens Use."

a. The forensic review of the cellular telephone showed that, during the above timeframe, A.G. viewed Craigslist advertisements for the sale of "roofing tar" associated with multiple seller identification numbers, including 6633650659.

b. The contents of A.G.'s phone also show that in the same timeframe, July 3, 2018, A.G. communicated with a dealer (later identified as Andrew MADI) via multiple cellular text messages; MADI used the telephone number (213) 237-1587 (the "1587 phone number"), which showed among other things the following:

i. MADI stated that he was out of roofing tar but had some "China White" and that he had a money back guarantee if A.G did not like it. MADI also stated that a half of a gram lasts him a week. MADI stated that he would only go forward with the transaction after reviewing A.G.'s social media profile (i.e., as a method of detecting whether A.G. was an undercover law enforcement officer), following which they arranged to meet at the Whole Foods Market located at the shopping center at the intersection of Fairfax Avenue and Santa Monica Boulevard in West Hollywood, California to complete the transaction. MADI said he is a computer technician and was currently at work. (MADI's place of employment, Stan's Tech Garage 7867 1/2 Santa Monica Blvd, West Hollywood, CA, is located in a shopping center that also houses a Whole Foods Market; the Fairfax/Santa Monica intersection is the center's southeast corner.) MADI said that he had ".65" ready which I believe referred to a .65 gram quantity of "China white" heroin.

ii. Upon A.G.'s arrival, MADI directed A.G. to the area behind the Chinese restaurant because he (MADI) was at work (i.e., at Stan's Tech Garage) and did not want to get caught doing this at work. (There is a Chinese restaurant, Kung Pao Bistro, is also located in the same shopping complex that houses Stan's Tech Garage)

iii. Hours later, MADI contacted A.G. via text message and asked how A.G. was doing. A.G. responded that it was "pretty powerful." A.G. stated that he preferred the "slow casual smoking of tar" and noted that "this white does the job that's for sure." MADI said that he was the same way and that he (MADI) likes the China white because "you have to smoke less of it to get high." They discussed the difference in how the tar and China white "slide" or smoke when heat is applied. MADI gave A.G. a tip in how to smoke the China white stating, "Gotta use heavy duty foil and flatten it really good with like the side of a lighter or something. Make sure it is perfectly flat and smooth and it slides like a champppp."

c. The forensic analysis of A.G.'s phone also showed that A.G. reached out via text message to other suspected heroin dealers (i.e., based on other Craigslist advertisements that A.G. found), but found no other reply communications to A.G.'s text messages prior to the above transaction with MADI. One dealer sent a message on July 3, 2018 (after A.G. had purchased drugs from MADI, based on the above exchange) asking if A.G. still needed anything; A.G replied that he did not but would contact the dealer in the future.

2. Surveillance at the Whole Foods Market in West Hollywood and the identification of MADI

11. I conducted a Google search of the Whole Foods Market at the intersection of Fairfax Avenue and Santa Monica Blvd. in West Hollywood, CA. I saw, from the Google maps images, that the Whole Foods Market was part of a larger business complex with multiple businesses, one of which is Stan's Tech Garage.

12. On July 12, 2018, beginning at approximately 10:30 to 11:00 a.m., DEA agents established surveillance at Stan's Tech Garage.

a. During the course of the surveillance operation, agents observed a tall, thin male wearing what appeared to be a Stan's Tech Garage shirt emerge from the business on multiple occasions. Agents queried the publicly available Facebook page for Stan's Tech Garage and located the page of Stan Katz, owner of the business. On examining Katz's Facebook "friends," agents located the Facebook page for MADI. Agents observed that the publicly available profile photo of MADI on his Facebook page matched the person agents observed at the store. Agents also obtained MADI's California driver's license photo, which they recognized likewise matched the person they had seen (and also MADI's Facebook profile photo).

b. At approximately 12:30 p.m., Agent's observed MADI in front of the door of Stan's Tech Garage meeting with an unidentified female ("UF1"). UF1 gave MADI a thermal cup, and agents then saw MADI appear to place an object inside the cup and return it to UF1. I believe this interaction was a

concealed hand-to-hand drug transaction. From my training and experience, including from my experience buying user amounts of heroin in an undercover capacity, I know that dealers often seek to conceal drugs that are being sold to a customer, and I believe that placing the drugs into a thermal cup was such a means of concealing the contraband being exchanged. I also know from my training and experience that drug traffickers and users will frequently use cups for such concealed transactions, as the cups can be discarded without arousing suspicion in the event that law enforcement is seen nearby. UF1 then left the area on foot. She was observed returning again that evening wearing a Stan's Tech Garage shirt, and MADI left Stan's Tech Garage on foot a short time later.

c. Agents maintained surveillance on MADI as he walked into a convince store. When MADI emerged, he approached one of the agents on surveillance. MADI asked the Agent to "take a walk" with him. MADI told the agent that he (the agent) was outside of his (MADI's) work all day. The agent denied the allegation, and the surveillance was terminated. I believe that MADI asked to "take a walk" with the agent to determine whether the agent was interested in purchasing drugs, and thus that MADI did not know that the agent was a law enforcement officer.

13. Following the surveillance operation, I conducted law enforcement public records database queries regarding MADI. I observed that, at that time, MADI was listed as residing at 329 North Ogden Street Los Angeles, CA. (For the reasons discussed

herein, I submit that, a few months earlier, MADI had moved from that residence to SUBJECT LOCATION 1.)

3. Information from Craigslist

14. As discussed above, forensic review of A.G.'s cellular telephone reflects that he obtained the fentanyl that caused his overdose death after conducting Craigslist searches advertising the sale of heroin, including a posting from a seller associated with identification number 6633650659. I served a subpoena on Craigslist for, among other things, records associated with recent postings by any person using the 1587 phone number (the phone number used by MADI to coordinate the transaction with A.G.), and all associated postings for the months June 2018, July 2018, and August 2018. Craigslist provided responsive records to me on August 16, 2018.

a. The records from Craigslist include postings associated with seller identification number 6633650659, created on July 3, 2018, by a user associated with the 1587 phone number, stating the following: "I own a roofing company. I have roofing tar and china roofing plates for sale, top quality you will not be disappointed or your money back guaranteed. Also have quality green ladders as well, very sturdy and reliable, no problem getting you high up so you can get your work done Text for more information." From my training and experience, I recognize this post as a coded offer to sell black tar heroin ("roofing heroin") or china white heroin ("china roofing plates"). I believe that the term "green ladders" was code for other drugs being offered for sale, and I know that prescription

pills of Xanax (generic name alprazolam, a Schedule IV benzodiazepine and popular black market drug) are sometimes referred to as "ladders" because of their rectangular shape and etching resembling a ladder. I believe that "green ladders" is code for the green-colored preparation of alprazolam (or of a similar drug such as a designer benzodiazepine counterfeited to appear like alprazolam).

b. The Craigslist records also show that the email address associated with account for the user of the 1587 phone number is darknetstuff9115@gmail.com.

i. Regarding the email address darknetstuff9115@gmai.com, from my training and experience, I know that the "dark net," also sometimes called the "dark web" 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 and other encryption technologies, to ensure that communications and transactions are shielded from interception and monitoring.

c. Additionally, the records from Craigslist show that the MADI (i.e., the person using the 1587 phone number and the darknetstuff9115@gmail.com email address) had also posted two earlier coded advertisements for the sale of heroin:

i. A posting created on June 17, 2018, stating: "I own a roofing company and antique shop. I have roofing tar and china plates for sale, top quality you will not be disappointed or your money back guaranteed. Text two1three two3seven 15eight7"

ii. A posting created on July 2, 2018, stating: "I own a roofing company and antique shop. I have roofing tar and china plates for sale, top quality you will not be disappointed or your money back guaranteed. Green ladders as well just ask about them Text two1three two3seven 15eight7"

(I) Here again, I recognize the references to "roofing tar", "china plates", and "green ladders" to be code for black tar heroin, china white, and Xanax respectively. Likewise, I believe the reference to "top quality" is a coded reference to high purity of the drugs offered for sale. I also recognize that the statement "Text two1three two3seven 15eight7" is a coded reference to the 1587 phone number ((213) 237-1587).

15. Craigslist captures the Internet Protocol ("IP") address of the poster. (An IP address is an identification number assigned to hardware used by computers or other electronic devices such as cellular telephones to connect to the internet.) The IP address of the July 3 posting (i.e., the one believed to have resulted in the sale to A.G.) is 107.184.250.7, and I saw that the IP address for the June 17 posting is 76.168.142.66. I conducted an open-source internet search of those IP addresses and learned that they are serviced by the internet provider Charter Communications. I served Charter with

a subpoena requesting subscriber records for the IP addresses during the respective postings.

a. I received records from Charter showing that IP address 107.184.250.7 was subscribed to Stan's Tech Garage at 7867 1/2 Santa Monica Blvd in West Hollywood, CA (hereafter, the "STAN'S TECH GARAGE IP address").

b. The records also show that IP address 76.168.142.66 was subscribed to Emily Greenberg of 329 North Ogden Avenue in Los Angeles, CA (hereafter, the "329 North Ogden IP address 1"). This is the same address for MADI shown in the public records queries that I conducted after MADI was observed during the July 2018 surveillance at Stan's Tech Garage.

16. I conducted searches of MADI's publicly available Instagram and Facebook profiles. I observed that MADI and a person named Emily Greenberg are "followers" of each other's Instagram pages. Additionally, MADI is "friends" on Facebook with a person named Emily Greenberg, whose profile picture matches the user of the Emily Greenberg Instagram account.

4. Information pertaining to the 1587 phone number

17. During the investigation, I learned that the 1587 phone number is serviced by Onvoy, LLC doing business as Inteliquent ("Inteliquent"). I served a subpoena on Inteliquent for records including subscriber information and call detail records ("CDR") for the 1587 phone number. On July 12, 2018, Inteliquent responded, among other things, that the 1587 phone number "is assigned to the following wholesale customer: TextMe, Inc."

a. TextMe is a third party communications phone application that allows users to select a phone number and use that number to send and receive telephone calls and text messages as one would with a standard cellular telephone; users can change numbers at any time. From my training and experience, I know that drug traffickers will commonly use such third party phone numbers as "burner" numbers that can be used to facilitate drug trafficking and other offenses to evade law enforcement detection.

b. I served TextMe with a subpoena for subscriber information and CDR data pertaining to the 1587 phone number. On July 17, 2018, TextMe responded to the subpoena providing the requested information, showing that the 1587 phone number was subscribed to username darknetstuff91158599 (i.e., a username similar to the darknetstuff9115@gmail.com e-mail address shown on the Craigslist records discussed above); that the account was created on June 17, 2018; and that the account user's e-mail address is darknetstuff9115@gmail.com. TextMe offered a caveat that the above e-mail address was provided by the user and is not independently verified by TextMe.

c. TextMe also provided CDR for the 1587 phone number. Because the service is internet based, TextMe records the IP addresses for outgoing messages. I isolated the outgoing messages to A.G.'s phone from the CDR records and noted two unique IP addresses for those messages. One is the STAN'S TECH GARAGE IP address. The other was an IP address associated with a Sprint Wireless account, which led me to believe that MADI

uses a Sprint-serviced cellular telephone. Sprint does not retain IP address data for their wireless customers. However, I served Sprint with a subpoena seeking any accounts associated to MADI, and learned that MADI has at least two Sprint telephones in his name, however only one was active at the time of the July 2018 drug sale to A.G. The phone number that was active and subscribed to MADI is 949-842-6138 ("MADI's Telephone").

d. In addition to the IP addresses associated with text messages, TextMe records IP addresses when accounts are established. The IP address when the account for the 1587 number was established on June 17, 2018 was 76.168.112.85. I subpoenaed Charter for records associated with the 76.168.112.85 IP address at that time, and the responsive records showed that it was subscribed to Greenberg at the 329 North Ogden address (hereafter, the "329 North Ogden IP address 2").

e. According to the TextMe records, the 1587 number was last used on July 13, 2018. The show the last IP address was 172.88.105.168. I subpoenaed Charter communications for subscriber information pertaining to 172.88.105.168 between June 1, 2018 and September 19, 2018. The responsive records show that the IP address is subscribed to Kayla Kinsey at SUBJECT LOCATION 1 (855 North McCadden Place in Los Angeles, CA). Hereafter, IP address 172.88.105.168 is referred to as the "SUBJECT LOCATION 1 IP address."

5. Further investigation regarding MADI's connection to Kinsey and to SUBJECT LOCATION 1

18. During the course of this investigation, I queried Los Angeles Department of Water and Power ("LADWP") for 329 North Ogden Street. I observed that utilities were paid by Kayla Kinsey until approximately July 6, 2018, following which Kinsey left a forwarding address of SUBJECT LOCATION 1 (855 North McCadden Place in Los Angeles, CA).

19. I also searched MADI's publicly available Facebook and Instagram profiles for evidence of his connection to Kinsey. I found Instagram and Facebook profiles for a person named Kayla Kinsey, which bore profile photos matching the Kinsey's California driver's license photo. I observed that MADI and Kinsey follow each other on Instagram and are "friends" on Facebook. Additionally, I saw pictures of MADI and Kinsey posing together on MADI's Instagram profile, including in a photo posted on December 3, 2017 and another photo posted on August 26, 2018. The latter photo included caption that the photo was taken at Joshua Tree House, a rental house near Joshua Tree National Park. Accordingly, I believe that MADI and Kinsey are a romantic couple, and that they share use of SUBJECT LOCATION 1. Moreover, as discussed in more below, surveillances and GPS data for MADI's cellular telephone verify his frequent presence at SUBJECT LOCATION 1, including during the night, and IP Address data likewise corroborates that MADI frequently uses the internet at that location.

6. Information from Google pertaining to darknetstuff9115@gmail.com.

20. On August 16, 2018, the Hon. Michael R. Wilner, United States Magistrate Judge, signed a search warrant for Google records associated with darknetstuff9115@gmail.com.

a. I received the records from Google in response to the warrant, including emails and an activity log. The emails included communications dating from March, June, and July 2018 that I recognize advertised the sale of controlled drugs, including "roofing tar" (heroin), "china plates" ("china white" heroin and fentanyl) and "white X3 ladders" (Xanax). The emails also included communications with TextMe and another third party text messaging service, Pinger, referring to three different phone numbers used by MADI other than the 1587 phone number; I thus believe that MADI uses multiple different third party messaging services to conceal his online trafficking. Notably, multiple communications were addressed to "Andrew," which is MADI's first name.

b. Another email from the account was sent from MADI to himself attaching a Pretty Good Privacy ("PGP") encryption key. PGP is an online encryption program commonly used by black market traffickers to, for example, encrypt incriminating communications. I know from my training and experience that traffickers using the dark web to buy and sell drugs commonly use PGP encryption to protect their communication from law enforcement detection.

c. I also know that such traffickers will sometimes decrypt messages and email such messages to themselves for future reference. I noted what I believe to be such a decrypted e-mail message, dated March 10, 2018. The message appears to be a review free sample of 2-mg white Xanax pills from "thefastplug", a vendor on Dream Market. Dream Market is a dark web marketplace on which people order illegal drugs, stolen property, and other illegal contraband. The buyers pay with bitcoin or other cryptocurrency and the drugs are discreetly shipped to their door. In June 2018, Jose Robert Porras III, a dark web vendor using the alias "thefastplug," was indicted in the Eastern District of California as part of Operation Dark Gold, a law enforcement sweep targeting dark web vendors across the United States. Porras was charged with distribution of drugs including Xanax via Dream Market and other dark web marketplaces, and with laundering the proceeds of such trafficking via Bitcoin transactions. I thus believe that MADI utilizes the dark web to acquire drugs (as corroborated by MADI's use of the handle "darknetstuff"), and that related evidence will be found on computers and storage devices within the SUBJECT LOCATIONS.

d. I did not observe any communications of a personal nature in the search warrant records from darknetstuff9115@gmail.com. From my training and experience, I recognize that darknetstuff9115@gmail.com was a "burner" account used by MADI to facilitate online trafficking on a short-term basis; I submit this is corroborated by other apparently

personal e-mail addresses used by MADI that I have observed from various subpoenaed records, as discussed below. Given the facts herein reflecting MADI's sophisticated means of concealing his trafficking, including rotating between "burner" phone numbers and use of PGP encryption, I believe that MADI also rotates between "burner" email accounts, and darknetstuff9115@gmail.com was one such account used between March and July 2018.

21. The Google search warrant return also showed several IP addresses associated with various account activities to include account logins/logouts, Google search queries, and Google maps queries and activities.

a. The IP address used to agree to the Google terms of service was the STAN'S TECH GARAGE IP address. (The account was established on March 8, 2018.) From April 4, 2018 to August 15, 2018, there were thirteen logins from the STAN'S TECH GARAGE IP address. On June 20 2018, there were two logouts from the STAN'S TECH GARAGE IP address. Thus, I believe that the Google account darknetstuff9115@gmail.com was used multiple times by internet enabled devices such as computers or phones at Stan's Tech Garage, including activation of the account.

b. I reviewed the activity log of the account. Google provided a total of 2,447 activity records for the account for July 16, 2018 to August 16, 2018. The activity log provides data including the date, time, IP address, and type of service used. I isolated the activities by IP address and observed 358 activities originating from the SUBJECT LOCATION 1

IP address, and 250 activities originating from the STAN'S TECH GARAGE IP address.

c. The activity log records also provided information as to what application was being used to access the Google account. The information showed that the applications were being accessed by an Apple computer and an Apple iPhone.

22. In addition to the search warrant signed August 16, 2018, I obtained a follow-up search warrant seeking internet search history for darknetstuff9115@gmail.com, which was signed on September 25, 2018 by the Honorable John E. McDermott, United States Magistrate Judge, Central District of California.

a. The responsive records show that, on June 17, 2018 at approximately 3:24 p.m., MADI made two queries for driving directions from SUBJECT LOCATION 1 to the intersection of Buckingham Road and Jefferson Blvd in Los Angeles, and another query for directions from Stan's Tech Garage to the same intersection. As noted, this is the same date on which MADI had created the 1587 number via TextMe, and Craigslist records show that MADI posted an advertisement for "top quality" "roofing tar and china plates" (black tar heroin and china white fentanyl/heroin, respectively) two hours earlier at approximately 1:40 p.m. Accordingly, I believe that MADI was arranging to conduct a drug transaction at that location, and he was pulling up driving records from both SUBJECT LOCATION 1 and Stan's Tech Garage to be prepared to travel to that location to complete the sale.

b. The search history also showed that, on July 14, 2018, MADI searched for "free texting number," and ran queries for pricing of prepaid phones and phone plans on July 14, 2018, which I submit further corroborates that MADI continued to use "burner" phone numbers to engage in online trafficking even following A.G.'s overdose death. The records showed that MADI conducted multiple searches for "Ketamine Clinics of Los Angeles" on June 17, 2018 (Ketamine is a Schedule III prescription controlled substance that is commonly abused on the black market), and that minutes later he reviewed an article entitled "US Ketamine Clinics Continue to Mushroom With No Regulation." From an open source internet search, I observed that Ketamine Clinics of Los Angeles is the name of a medical facility in West Los Angeles. MADI also searched for "deposit cash chime" in June 2018; Chime Banking is an online banking platform. As noted below, I have obtained records from Bancorp, which controls Chime Banking, verifying that MADI in fact has such an account.

7. Information from Coinbase

23. I served a subpoena to Coinbase, a money transfer service facilitating the purchase, sale and use of cryptocurrencies such as Bitcoin. I know from my training and experience that dark net vendors who illegally sell drugs online, such as "thefastplug," often utilize Bitcoin and other cryptocurrencies as payment, in an attempt to conceal the transaction from law enforcement.

a. I received responsive records through approximately October 15, 2018, which show that a Coinbase account was established in MADI's name at his father's address in San Clemente on February 2, 2018, with the e-mail address andrewjmadi@yahoo.com. The bank account associated to the Coinbase account is a Chime Banking account; as noted above, the search results from darknetstuff9115@gmail.com included a query regarding depositing funds into a Chime account.

b. The response also provided an events log listing the activity of the account and the IP address associated with the activity, which showed:

i. Twenty-three entries from the 329 North Ogden Street IP address 2, on May 7, 2018.

ii. Five entries from the SUBJECT LOCATION 1 IP address, on June 23, 2018.

iii. Thirteen entries from the STAN'S TECH GARAGE IP address on August 22, 2018. (I submit that the continued cryptocurrency activity into late August 2018 further corroborates that MADI had continued to engage in online trafficking even after selling the fentanyl that caused A.G.'s overdose death.)

8. Information from Apple

24. I served a subpoena to Apple asking for account information pertaining to Apple ID account for among other things, MADI and/or darknetstuff9115@gmail.com. The responsive records showed that MADI had an Apple account, but that it was not with darknetstuff9115@gmail.com. (I submit this further

corroborates that the latter was a "burner" account used by MADI to facilitate online drug trafficking.) Notably, the e-mail address associated with MADI is 9andrew115@gmail.com. I noticed that the numbers "9115" also feature prominently in the darknetstuff9115@gmail.com e-mail address.

25. The Apple iTunes subscriber information for MADI show that the account registered to MADI at 329 North Ogden Street in Los Angeles, CA. I also received IP address information associated with access to the iTunes account, which showed among other things:

a. There were 214 entries from the 329 North Ogden Street IP Address 2 from November 10, 2017 to June 19, 2018.

b. There were 20 entries from the SUBJECT LOCATION 1 IP address from June 20, 2018 to August 21, 2018. (I submit that this further verifies that that MADI moved from 329 North Ogden to SUBJECT LOCATION 1 on or about June 20, 2018.)

c. There were 57 entries from the STAN'S TECH GARAGE IP address from February 8, 2018 to September 11, 2018.

d. I also submit that the above corroborates MADI's use of the 1587 number, Craigslist account, and "burner" email account (darknetstuff9115@gmail.com), given the substantial overlap in IP addresses with MADI's personal Apple account, and I also note the substantial overlap in access to such accounts from both of the SUBJECT LOCATIONS.

9. Surveillance at SUBJECT LOCATION 1 on August 9, 2018

26. On August 9, 2018, beginning at 8:30 a.m., I and other investigators conducted surveillance at 855 North McCadden Place (SUBJECT LOCATION 1). SUBJECT LOCATION 1 is an apartment within a four-unit complex. Within five minutes of establishing surveillance, SA Tony Bliss observed MADI emerge from the north side of the apartment complex. Agents were not able to follow MADI due to heavy morning traffic.

27. After the surveillance operation, I checked the LADWP utility records of the four units within the building, 853, 853 1/2, 855, and 855 1/2 North McCadden Place. Neither MADI or Kinsey were listed as paying utilities at any of the units. I observed that a person named "Anne King" is the listed subscriber for utilities at 855. The record lists (339) 222-9062 as King's phone number. I checked phone number 339-222-9062 in the publicly available search function within the Facebook Messenger application (a communications platform for Facebook users), which resulted in displaying a Facebook profile for a person named Anne King. I searched King's publicly available Facebook profile for and observe that she is "friends" with both MADI and Kinsey. King also has an Instagram account with a recent photo including her and Kinsey.

10. GPS tracking warrant following identification of SUBJECT LOCATION 2

28. In late October, investigators learned from California DMV records that, on October 16, 2018, MADI changed the address

associated with his driver's license to SUBJECT LOCATION 2 (115 South Commonwealth Avenue in Los Angeles, CA).

29. On October 25, 2018, the Honorable Alka Sagar, United States Magistrate Judge, signed a warrant (18MJ02822) authorizing the GPS tracking for MADI's cellular telephone (949-842-6138) for a period of 45 days. I began receiving GPS data beginning that evening, in 15 minute intervals.[1] As of November 26, 2018 at approximately 4:01 p.m., I have received approximately 2877 total locational records in response to the warrant.

a. Of the 2877 results, 665 show MADI to be at SUBJECT LOCATION 1, including that MADI frequently stays at SUBJECT LOCATION 1 overnight, most recently on November 18 to November 19, 2018.[2]

b. 1362 of the pings are to SUBJECT LOCATION 2.[3] Here again, the pings show that MADI also regularly stays overnight at SUBJECT LOCATION 2, most recently from November 23 to November 24, 2018. Given the frequent pings to SUBJECT LOCATION 2, including overnight, and the recent address change

---

[1] From approximately November 24, 2018 4:38 p.m. PST to November 26, 2018 11:05 a.m. the disclosure of the GPS information was inadvertently stopped by Sprint and no GPS information was collected during that time.

[2] When Sprint provides the GPS data, they provide data including the date and the time of the coordinate, a latitude and longitude coordinate, and an estimate of the accuracy of the coordinate measured. The coordinate provided for SUBJECT LOCATION 1 has an accuracy of approximately 1058 meters.

[3] The coordinate provided by Sprint for SUBJECT LOCATION 2 has an accuracy of approximately 644 meters.

to MADI's address in California DMV records, I believe that MADI also resides at SUBJECT LOCATION 2.

11. Surveillances in October/November 2018

30. On October 31, 2018 at approximately 11:15 a.m., investigators established surveillance at SUBJECT LOCATION 1. The pings described above indicated that MADI was at the location. At approximately 1:30 p.m., SA James Young and SA LaShay Thomas approached SUBJECT LOCATION 1 and knocked on the door. MADI answered the door. SA Young and SA Thomas performed a ruse and claimed that they were looking for a lost dog. MADI said that he had been there all day and had not seen their dog. SA Young and SA Thomas then left the area and surveillance was terminated.

31. Investigators have conducted surveillance at SUBJECT LOCATION 2 on two occasions, October 23, 2018 from approximately 4:00 p.m. to 6:30 p.m., and on October 24, 2018 from approximately 10:00 a.m. to 12:00 p.m. Investigators did not see MADI during the former. During the latter, DEA SAs Tony Bliss and Matt Lozowski rang the doorbell by the driveway gate for the residence. An elderly female spoke to them through a partially open front window near the driveway gate. SAs Bliss and Lozowski conducted a ruse that they were looking for an apartment to rent. The female said that there were no apartments at the site and that her house was a single family residence. The elderly female used a stick to point to the large apartment building across the street and said that the apartments were over there.

32. Although California DMV records for MADI identify his address as SUBJECT LOCATION 2, based on the latter surveillance just noted, and in an abundance of caution, on November 26, 2018, investigators conducted a further surveillance operation to verify MADI's presence at SUBJECT LOCATION 2. At approximately 2:54 p.m. that day, MADI's cellular telephone pinged to the area of SUBJECT LOCATION 2. Agents arrived at the location at approximately 3:00 p.m. Shortly thereafter, at approximately 3:05 p.m., SA Bliss observed a Hyundai coupe bearing CA/7TVE003 (registered owner James A Dauterman at 1118 West 39th Place Los Angeles, CA 90037), and driven by an unidentified male, park in front of the driveway of SUBJECT LOCATION 2. Agents then saw MADI open the gate on the driveway leading to SUBJECT LOCATION 2 and enter the front passenger seat of the Hyundai coupe, after which the Hyundai coupe left the area. Surveillance was maintained for a short distance before the coup was lost in traffic. The next ping for MADI's cellular telephone was received at 3:11 p.m., and showed that MADI's phone had left the area of SUBJECT LOCATION 2, which I submit corroborates the investigators' observations during the surveillance operation.[4]

---

[4] Investigators do not presently know whether MADI uses the entire residence or is merely renting a particular room/area within SUBJECT LOCATION 2. However, on executing the search warrant for SUBJECT LOCATION 2 sought herein, should investigators identify any room(s) controlled exclusively by a third party and is not otherwise used by MADI, investigators will terminate any search of such room(s).

12. Information from Chime Bank

33. In October 2018 I served Bancorp, the parent company of Chime Bank with an Grand Jury Subpoena requesting banking records. The responsive records included bank documents from January 1, 2017 to November 6, 2018. The address listed for MADI is 115 South Commonwealth Avenue, Los Angeles, CA (SUBJECT LOCATION 3 CV). The records also showed MADI's previous address of 329 North Ogden Street Los Angeles, CA.

13. Information regarding MADI's Sprint-Serviced Cellular Telephone

34. On or about November 18, 2018, I served a subpoena to Sprint for MADI's cellular telephone, 949-842-6138. According to the responsive records, I learned the following:

a. The account was established October 25, 2017 and was active through the date searched (November 18, 2018).

b. The records included CDR (call detail records) which show a continuing pattern of incoming and outgoing calls and text messages from MADI's cellular telephone, which I submit corroborates that it is still in use by MADI. (I further submit that this is corroborated by the November 26, 2018 surveillance discussed above showing locational data for that cellular telephone tracking MADI's approximate whereabouts.)

c. MADI's cellular telephone (i.e., the cellular device for phone number 949-842-6138) bears Electronic Serial Number ("ESN") 310120218357159 effective October 25, 2017 and was through the most recent data (November 18). From my training and experience, I know that an ESN is a unique number

assigned to a cellular telephone and that, before a call is made, the phone transmits the ESN to the mobile carrier's base station. The base station will then check to see if that ESN is authorized to use that network. Because the ESN of the phone was effective October 25, 2017 and has not changed through the most recent data, I believe that MADI has been using the same phone since October 25, 2017 to the present date.

d. As discussed above, the fentanyl transaction between A.G. and MADI occurred via a third party text messaging service, TextMe, and records from TextMe verify that the user of the service (i.e., MADI) utilized a Sprint phone. Accordingly, I further believe that MADI used the same cellular telephone currently in his possession to negotiate the fentanyl sale to A.G. that ultimately caused A.G.'s overdose death. I likewise believe that MADI used the same cellular telephone to engage in other drug transactions with his online black market customers, via the same TextMe phone number and the other rotating "burner" third party text messaging phone numbers that he has utilized.

14. Summary Regarding SUBJECT LOCATIONS

35. In summary, I submit that the evidence set forth above demonstrates probable cause that MADI resides at both SUBJECT LOCATIONS 1 and 2, interchangeably. Moreover, I submit that the discussion above regarding the SUBJECT LOCATION 1 IP Address demonstrates that MADI utilizes SUBJECT LOCATION 1 to access "burner" phone numbers and email addresses (including the 1587 phone number and the darknetstuff9115@gmail.com email address) that MADI uses for drug trafficking, and that MADI utilized his

prior residence (329 North Ogden Street) and workplace (Stan's Tech Garage) to do the same, thus further generally corroborating that MADI engages in online drug trafficking out of his residence and other locations that he frequents. Although I believe that MADI also sold drugs out of Stan's Tech Garage for the reasons discussed herein, I submit that it is unlikely that MADI permanently stored drugs at that location, given that he is merely employed there and to my knowledge does not otherwise own or control the business or its premises. Moreover, I believe that MADI no longer works at that business: according to the business's website, as GPS data for MADI's cellular telephone shows that he no longer travels to that location. Accordingly, I submit that there is probable cause that evidence that will be found at the SUBJECT LOCATIONS include both computer/digital evidence regarding MADI's online trafficking, and also controlled drugs and other contraband.

36. Additionally, I submit that the foregoing facts demonstrate that MADI has been involved in longtime online drug trafficking, involving multiple types of substances. I also know from my conversations with Assistant United States Attorney ("AUSA") Benjamin R. Barron that the case law in the Ninth Circuit establishes a general presumption that individuals involved in drug trafficking conspiracies, including their assistants, maintain evidence of these crimes in their residences. AUSA Barron provided me the following case citations: "In the case of drug dealers, evidence is likely to be found where the dealers live." United States v. Angulo-

Lopez, 791 F.2d 1394, 1399 (9th Cir. 1986) (citations omitted). "When the traffickers consist of a ringleader and assistants, a fair probability exists that drugs will be present at the assistants' residence as well as the ringleader's." Angulo-Lopez, 791 F.2d at 1399 (citations omitted). "[E]vidence discovered by [] officers linking the defendants to a drug scheme provide[s] 'more than a sufficient showing for obtaining the warrant to search [their] ... residence.'" United States v. Fannin, 817 F.2d 1379, 1382 (9th Cir. 1987) (quotation and citation omitted).

IV. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

37. 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. Based on my knowledge, training, and experience, as well as information related to me by agents and

others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A

single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet.[5] Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before

[5] These statements do not generally apply to data stored in volatile memory such as random-access memory, or "RAM," which data is, generally speaking, deleted once a device is turned off.

they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital 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 contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was

ATTACHMENT A

once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data

on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

g. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime. In addition, decryption of devices and data stored thereon is a constantly evolving field, and law enforcement agencies continuously develop or acquire new

methods of decryption, even for devices or data that cannot currently be decrypted.

38. Based on the facts discussed above, and based on my training and experience I believe that digital devices will be found during the search, to include Apple devices. For example, as discussed above, the Google records show that MADI accessed darknetstuff9115@gmail.com from both an Apple iPhone and an Apple computer, and the Apple records for MADI's account discussed above likewise verify that he uses an iPhone and other Apple services such as iTunes.

a. I know from my training and experience and my review of publicly available materials that several hardware and software manufacturers offer their users the ability to unlock their devices through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint-recognition, face-recognition, iris-recognition, and retina-recognition. Some devices offer a combination of these biometric features and enable the users of such devices to select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple Inc. ("Apple") offers a feature on some of its phones and laptops called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the

relevant finger to the device's Touch ID sensor, which on a cell phone is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the phone, and on a laptop is located on the right side of the "Touch Bar" located directly above the keyboard. Fingerprint-recognition features are increasingly common on modern digital devices. For example, for Apple products, all iPhone 5S to iPhone 8 models, as well as iPads (5th generation or later), iPad Pro, iPad Air 2, and iPad mini 3 or later, and MacBook Pro laptops with the Touch Bar are all equipped with Touch ID. Motorola, HTC, LG, and Samsung, among other companies, also produce phones with fingerprint sensors to enable biometric unlock by fingerprint. The fingerprint sensors for these companies have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. To activate the facial-recognition feature, a user must hold the device in front of his or her face. The device's camera analyzes and records data based on the user's facial characteristics. The device is then automatically unlocked if the camera detects a face with characteristics that match those of the registered face. No physical contact by the user with the digital device is necessary for the unlock, but eye contact with the camera is often essential to the proper functioning of these facial-recognition features; thus, a user must have his or her eyes

open during the biometric scan (unless the user previously disabled this requirement). Several companies produce digital devices equipped with a facial-recognition-unlock feature, and all work in a similar manner with different degrees of sophistication, e.g., Samsung's Galaxy S8 (released Spring 2017) and Note8 (released Fall 2017), Apple's iPhone X (released Fall 2017). Apple calls its facial-recognition unlock feature "Face ID." The scan and unlock process for Face ID is almost instantaneous, occurring in approximately one second.

d. While not as prolific on digital devices as fingerprint- and facial-recognition features, both iris- and retina-scanning features exist for securing devices/data. The human iris, like a fingerprint, contains complex patterns that are unique and stable. Iris-recognition technology uses mathematical pattern-recognition techniques to map the iris using infrared light. Similarly, retina scanning casts infrared light into a person's eye to map the unique variations of a person's retinal blood vessels. A user can register one or both eyes to be used to unlock a device with these features. To activate the feature, the user holds the device in front of his or her face while the device directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data from the person's eyes. The device is then unlocked if the camera detects the registered eye. Both the Samsung Galaxy S8 and Note 8 (discussed above) have iris-recognition features. In addition, Microsoft has a product called "Windows Hello" that provides users with a suite of biometric features

including fingerprint-, facial-, and iris-unlock features. Windows Hello has both a software and hardware component, and multiple companies manufacture compatible hardware, e.g., attachable infrared cameras or fingerprint sensors, to enable the Windows Hello features on older devices.

39. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents.

40. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features have been enabled. This can occur when a device has been restarted or inactive, or has not been unlocked for a certain period of time. For example, with Apple's biometric unlock features, these circumstances include when: (1) more than 48 hours has passed since the last time the device was unlocked; (2) the device has not been unlocked via Touch ID or Face ID in eight hours and the passcode or password has not been entered in the last six days; (3) the device has been turned off or restarted; (4) the device has received a remote lock command; (5) five unsuccessful attempts to unlock the device via Touch ID or Face ID are made; or (6) the user has

activated "SOS" mode by rapidly clicking the right side button five times or pressing and holding both the side button and either volume button. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time. I do not know the passcodes of the devices likely to be found during the search.

41. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features (such as with Touch ID devices, which can be registered with up to five fingerprints), and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual who is found at the SUBJECT LOCATIONS and reasonably believed by law enforcement to be a user of the device to unlock the device

using biometric features in the same manner as discussed in the following paragraph.

42. For these reasons, if while executing the warrant, law enforcement personnel encounter a digital device that may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) compel the use of MADI's thumb- and/or fingerprints on device(s) seized from the SUBJECT LOCATIONS pursuant to the instant warrants; and (2) hold the device(s) in front of the face of MADI with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature. With respect to fingerprint sensor-enabled devices, although I do not know which of the fingers are authorized to access any given device, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for fingerprint sensors; and, in any event, all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

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

///

V. CONCLUSION

44. For all the reasons described above, there is probable cause to believe that evidence of violations of 21 U.S.C. § 841(a)(1), (b)(1)(C) (distribution of controlled substances, including distribution resulting in death), 21 U.S.C. § 843(c) (advertising the sale of controlled substances via the internet), and 18 U.S.C. § 1956 (money laundering), as described above and in Attachment B of this affidavit, will be found in a search of the SUBJECT LOCATIONS, as further described above and in Attachments A(1) and A(2) of this affidavit.

Charles Valentine
Special Agent
Drug Enforcement Administration

Subscribed to and sworn before me on November 29, 2018.

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A